

Apr 2000

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-3511

**A National R&D Institute for Information
Infrastructure Protection (I3P)**

David R. Graham, Project Leader

Gregory J. Ayres

William J. Barlow

James P. Bell

Robert Bovey

Robert P. Hilton

Julie Consilvio Kelly

Charles H. Lyman

Michael S. Nash

Grant A. Sharp

Caroline F. Ziemke

Contributors:

Michael Leonard

W. T. Mayfield

Julian Nall

Robert E. Roberts

John R. Shea

Shelley D. Smith

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20000501 128

JO-5-1884

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE April 2000		3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE A National R&D Institute for Information Infrastructure Protection (I3P)			5. FUNDING NUMBERS DASW01-98 C 0067 AJ-6-1770	
6. AUTHOR(S) David R. Graham, Gregory J. Ayres, William J. Barlow, James P. Bell, Robert Bovey, Robert P. Hilton, Julie Consilvio Kelly, Charles H. Lyman, Michael S. Nash, Grant A. Sharp, Caroline FI Ziemke Contributors: Michael Leonard, W. T. Mayfield, Julian Nall, Robert E. Roberts, John R. Shea, Shelley D. Smith				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 1801 N. Beauregard Street Alexandria, VA 22311			8. PERFORMING ORGANIZATION REPORT NUMBER IDA Paper P-3511	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of the Deputy Under Secretary of Defense (Science and Technology)/Information Systems Directorate 1777 N. Kent Street, Suite 9030 Rosslyn, VA 22209			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A Approved for Public Release Distribution Unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) This paper assesses the need to create a new research organization with the mission to identify and address vulnerabilities in the nation's information systems and networks. Despite the many recent initiatives in this area, a broad cross-section of experts agrees that such an organization—if properly structured—could substantially strengthen a range of needed functions. The paper describes these functions and the kind of organization the experts believe can best perform them.				
14. SUBJECT TERMS Information security, information assurance, critical infrastructure protection, cyberterrorism, cyber vulnerabilities, national infrastructure protection			15. NUMBER OF PAGES 184	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

PREFACE

This study was performed by the Institute for Defense Analyses for the Office of the Deputy Under Secretary of Defense (Science and Technology) through the Information Systems Directorate. The task was entitled "Organization for National Information Infrastructure Protection."

Dr. Charles J. Holland and Dr. Steven E. King of the sponsoring office provided guidance and oversight.

Mr. James Kurtz and Dr. Gregory Larsen of IDA reviewed the report. Review comments on Chapter 11 also were provided by Rick Yanuzzi of the CIA. Oversight and guidance were provided by Dr. Robert Roberts and Mr. Michael Leonard. Ms. Shelley Smith edited the manuscript.

CONTENTS

Summary	S-1
Introduction.....	1
Part I Experts' Views on the PCAST Proposal	
1. Background: The PCAST Proposal	1-1
2. The Experts' Views on the PCAST Proposal	2-1
A. Nature of the Challenge.....	2-2
B. What Is to Be Done?.....	2-4
C. Is a Laboratory the Best Organizational Approach?.....	2-5
D. If Not a Laboratory, Then What Kind of Organization?	2-6
1. A Private-Sector Institute.....	2-7
2. Strong Leadership, Lean Staffing, and Strategic External Relations	2-8
3. Stimulating Research Environment	2-9
4. Direct Partnership with Industry	2-9
5. Committed, High-Level Government Sponsorship	2-9
6. Adequate and Secure Funding	2-10
Part II Growing Awareness of Infrastructure Vulnerabilities	
3. Gaining an Understanding of Cyber Vulnerabilities.....	3-1
A. Background.....	3-1
B. Infrastructure Vulnerabilities and Networked Information Systems	3-3
C. Vulnerability of Automated Control Systems	3-4
D. Potential Threats.....	3-6
E. The Growing Body of Evidence on Vulnerabilities	3-8
4. Vulnerabilities in Key Sectors	4-1
A. Internet Service.....	4-1
1. Vulnerabilities of the Internet Itself	4-2
2. Dependence of Other Critical Infrastructure Sectors on the Internet.....	4-3
3. Vulnerabilities Resulting from Interconnection.....	4-5

B. Telecommunications	4-5
1. Existing Vulnerabilities	4-6
2. Future Vulnerabilities	4-8
C. Electric Power	4-9
1. System Description	4-9
2. Control Center Vulnerabilities	4-10
3. Other Vulnerabilities	4-11
D. Transportation	4-12
E. Financial Services	4-14
1. Core Payments Infrastructure	4-15
2. Banking Systems	4-16
3. Securities Market Systems	4-17
F. Vulnerabilities and the Research Agenda	4-18
Part III Functions Needed for Infrastructure Protection	
5. Functional Assessment: Overview	5-1
A. The Functional Areas	5-1
B. The Baseline Organizations	5-2
6. Research and Development	6-1
A. R&D Requirements	6-1
1. PCAST Proposal	6-1
2. IDA Interviews and Workshops	6-2
3. R&D Roadmaps	6-3
4. Needed R&D Functional Tasks	6-5
B. Existing R&D Activities	6-7
1. Government Infrastructure Protection R&D Activities	6-8
2. Department of Energy	6-12
3. Department of Commerce	6-13
4. National Science Foundation	6-15
5. Other Organizations	6-16
C. The Role of the I3P	6-1
D. External Relationships	6-19
7. Information Sharing	7-1
A. Need for Information Sharing Function	7-1
1. Background	7-1
2. Information Sharing Tasks	7-2

B.	Existing Information Sharing Activities.....	7-3
C.	The Role of the I3P.....	7-6
D.	External Relationships.....	7-7
8.	Product and Service Evaluation.....	8-1
A.	Need for Product and Services Evaluation Function.....	8-2
1.	PCAST Proposal.....	8-2
2.	Phase 1 Results.....	8-2
3.	Phase 2 Results.....	8-2
B.	Existing Activities.....	8-5
1.	U.S. Government.....	8-5
2.	BITS Laboratory.....	8-7
3.	Commercial Evaluation Services.....	8-8
4.	Evaluating Deployed Systems.....	8-9
5.	Professional Certification.....	8-10
6.	Standards Organizations.....	8-10
7.	Assessment of Existing Activities.....	8-12
C.	The Role of the I3P.....	8-14
1.	Harmonize Processes and Criteria Used by Overseers and Evaluators.....	8-14
2.	Facilitate Ongoing Work and Establishing New Capabilities, as Needed.....	8-15
3.	Fill Gaps in Evaluation and Standards Area Where Only the Institute Is Serviceable.....	8-15
4.	Oversee an R&D Program to Improve Test Methods and Develop Tools, Metrics, and Benchmarks.....	8-16
5.	Establish Linkages that Promote the Gathering and Sharing of Information.....	8-17
D.	External Relations.....	8-17
9.	Education and Training.....	9-1
A.	Education and Training Requirements.....	9-1
1.	IDA Interviews and Workshops.....	9-1
2.	Pipeline of Information Technology Workers.....	9-3
B.	Potential Remedial Measures.....	9-6
1.	Increase the Number of Information Security Professionals.....	9-6
2.	Establish a Pool of Qualified Instructors.....	9-9

C. Current Activities	9-14
1. Government Initiatives.....	9-15
2. Private Sector Activities.....	9-17
3. Functional Gaps	9-18
D. The Role of the I3P.....	9-18
E. Operational Models	9-21
Part IV Toward an Institute for Information Protection	
10. Evaluation of Alternative Structures.....	10-1
A. Programmatic Initiative.....	10-2
1. Coordination Activities.....	10-3
2. Functional Activities.....	10-4
3. Assessment.....	10-5
B. Mission-Focused Government Activity.....	10-8
1. Examples.....	10-8
2. Assessment.....	10-9
C. Private Sector Consortium.....	10-10
1. Examples.....	10-11
2. Assessment.....	10-12
D. The Case for the I3P	10-13
E. Conclusion.....	10-18
11. Concept of Operations	11-1
A. Mission	11-1
B. Tasks, Deliverables, Performance Measures	11-2
C. Structure	11-2
1. Staffing and Governance.....	11-5
2. External Relationships	11-7
D. Government Funding and Sponsorship	11-9
E. Alternative Structures.....	11-10
1. A Private Corporation: IN-Q-TEL	11-11
2. DoD Federally Funded Research and Development Centers (FFRDCs).....	11-13
3. A Public Corporation	11-14

F. Legal and Regulatory Issues	11-15
1. Acquisition Regulations	11-16
2.. Intellectual Property	11-16
3. Restrictions on the Participation of Foreign or Multinational Firms	11-17
4. Information Protection and the Freedom of Information Act	11-17
5. Antitrust	11-19
4. Liability	11-19

Appendixes

A. The PCAST Letter to President Clinton	A-1
B. Interview and Workshop Participants	B-1

Figures

1-1. PCAST's Proposed Organization	1-3
6-1. Critical Infrastructure Protection R&D Interagency Working Group	6-8
9-1. The I3P's Role in Education and Training	9-
11-1. The Institute's Structure and External Relationships	11-5

Tables

5-1. Functional Areas	5-2
5-2. Baseline Organizations	5-3
5-3. Organizations Reviewed in Each Functional Area	5-4
6-1. Roadmaps for Information Assurance R&D	6-4
6-2. Framework for Information Assurance Research	6-5
6-3. FY2000 Government Agency Budget Requests for Critical Infrastructure Protection R&D	6-7
6-4. Assessment of Existing R&D Activities	6-18
6-5. Needed R&D Functional Tasks	6-19
7-1. Needed Information Sharing Functional Tasks	7-3
7-2. Assessment of Existing Information Sharing Activities	7-5
8-1. Desiderata for a Product and Service Evaluator	8-3
8-2. Assessment of Existing Product and Services Evaluation Activities	8-13
8-3. Needed Product and Services Evaluation Functional Tasks	8-14

9-1. Sources of Information Technology Workers	9-4
9-2. Non-degree Programs	9-6
9-3. Assessment of Existing Education and Training Activities	9-19
9-4. Tasks and Related INIP Activities	9-20
10-1. Functional Assessment of the Institute versus Alternatives	10-14
10-2. Alternatives versus Management Criteria	10-16
11-1. Representative Institute Tasks, Deliverables, and Performance Measures.....	11-3

SUMMARY

This paper assesses the need to create a new research organization with the mission to identify and address vulnerabilities in the nation's information systems and networks. Despite the many recent initiatives in this area, a broad cross-section of experts agrees that such an organization—if properly structured—could substantially strengthen a range of needed functions. The paper describes these functions and the kind of organization the experts believe can best perform them.

The need to address vulnerabilities in the nation's infrastructure sectors was articulated by the President's Commission on Critical Infrastructure Protection (PCCIP) in its 1997 report. The Commission described the growing importance of information systems to such critical sectors as communications, energy, transportation, banking and finance, water supply, emergency services, and public health services.¹ In May 1998, Presidential Decision Directive 63 (PDD-63) directed implementation of many of the Commission's recommendations.

In December 1998, the President's Committee of Advisors on Science and Technology (PCAST), having reviewed the provisions of PDD-63, proposed that a new laboratory be established to focus on the research and development required to understand and address vulnerabilities in the nation's information infrastructure. The President agreed with the PCAST that information assurance creates unique R&D challenges but requested a review to determine whether creating a new laboratory offered the best approach to meeting those challenges. As a result, the Deputy Director, Defense Research and Engineering, tasked the Institute for Defense Analyses (IDA) to conduct an independent assessment of the PCAST proposal to create a new laboratory, and to develop and analyze additional organizational options.

¹ These are the infrastructure sectors identified in PDD-63 and differ only slightly from those considered by the PCCIP. See *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, Executive Office of the President, May 1998.

VULNERABILITIES AND CONCERNS

The proliferation of networked information systems for operational management and control has created a spectrum of new vulnerabilities. These include accidental failure, intentional physical and cyber attacks, localized disruptions that cascade through interconnected systems, surreptitious intrusion into data bases and control systems, and terrorist threats that hold infrastructure sectors hostage to widespread and sustained disruptions. Both governments and transnational groups are developing concepts and strategies for exploiting these vulnerabilities as means of asymmetric warfare designed to offset the United States' dominant military capabilities. A few may well be on the way to developing the capability to carry out such cyber attacks.

As yet, no one understands the vulnerabilities with sufficient clarity to identify all the steps necessary to protect the critical information infrastructure. What is clear, however, is that the United States must increase its efforts to understand and address information infrastructure vulnerabilities. If we don't, we risk having others exploit them. Because the potential consequences are of strategic importance for the United States, the need for this R&D is a national concern.

FINDINGS: WHY A NEW ORGANIZATION IS NEEDED

Our findings reflect interviews with more than 100 experts in government, industry, and academia and two workshops that brought together a number of these interviewees and other experts in the area. In addition, the review drew on a White House conference that included the President's Science Advisor, the National Coordinator for Critical Infrastructure Protection and Counterterrorism, PCAST members, and the Chief Technology Officers from fifteen information technology firms.

The principal finding is that a new R&D organization is needed. The nation requires a program of information assurance research spanning the critical infrastructure sectors, and this entails a unique set of functions that are not being provided by any existing organization. Moreover, no existing organization is situated to assume responsibility for building the partnerships necessary to integrate activities across functions, across infrastructure sectors, and between the government and private sectors. This unique role requires establishing a new organization rather than modifying, combining, or expanding existing organizations.

In considering the appropriate structure for such an organization, the review began with the PCAST's proposed structural model, but it also considered modifications to this

model, as well as alternative structures. Three modifications to the PCAST proposal were incorporated: (1) altering the leadership structure to more strongly emphasize the joint partnership of industry, government, and academia; (2) focusing the organization's functions more explicitly on integration and collaboration, and on research that is not competitive with ongoing commercial and government programs; and (3) limiting the new entity to a small core staff combined with a strong external program. The resulting organizational concept has come to be known as the Institute for Information Infrastructure Protection (I3P). The use of the term "institute" is intended to denote the breadth of the organization's roles, and its added focus on building partnerships rather than purely on executing an in-house technology development program.

Altogether, four structural alternatives are described, compared, and assessed in Chapter 10:

- The I3P-- the PCAST's proposal for a government-funded private-sector organization with modifications as described above,
- a programmatic initiative -- expanded funding for current efforts within existing organizations.
- a new, mission-focused government agency or office, and
- a purely private sector consortium.

As discussed in Chapter 10, each of these approaches has support among some experts, and each brings certain strengths and weaknesses. On balance, however, we found general agreement that the I3P provides the best approach for building needed partnerships among the government, industry, and the private sector. This is especially important in establishing an effective framework for the information sharing essential for shaping and executing the R&D program. As a private sector entity, the I3P also offers the best way to attract an effective CEO and, by offering competitive salaries, to build the needed core technical staff. Finally, most experts believe a private institute such as I3P could most effectively formulate and manage the needed R&D program, because it can operate at "Internet speed" and adopt a culture compatible with the business community. The remainder of this summary focuses on the I3P model.

MISSION

The PCAST defined the basic purpose for a new organization. It is "to conduct research and develop technology that would protect our critical information and communications systems from penetration and damage by hostile foreign national or sub-national groups, organized crime, determined hackers, and from natural instabilities,

internal design weaknesses or human failings that can cause major disruption of highly complex, nonlinear networks.”

In addition, the I3P should be given the responsibility to help build the partnerships needed to integrate and coordinate ongoing activities. It must not only forge a national R&D agenda, but also perform the other closely related functions necessary for understanding and addressing infrastructure vulnerabilities. The draft mission statement below emphasizes the breadth of the technical challenge, and the recognized need to formulate and execute the program through partnerships among the involved communities:

Engage with industry, academia, and government to coordinate a national R&D program and related functions with the objective of avoiding disruptions of cyber systems that could result in catastrophic failures of the critical information infrastructure. In particular, emphasize R&D to understand vulnerabilities in the critical information infrastructure and develop counters to a widespread, well-organized attack that could severely disrupt or damage critical systems that are essential to our national defense, economic prosperity, and quality of life.

FUNCTIONS

The review identifies four functional areas where greater effort is needed to strengthen infrastructure protection. The I3P would not address all the observed shortcomings; nevertheless, it would play at least a supporting role in each of the areas.

Research and development

The main function of the new organization would be to identify, coordinate, integrate, and fund research directed toward understanding and ameliorating infrastructure vulnerabilities. Emphasis would be given to broad “systems-of-systems” problems with risks of large-scale consequences that cut across sectors and industries.

The initial R&D agenda should support development and integration of a national information infrastructure protection R&D strategy, and identify grand challenges. Representative challenge areas include:

- Understanding complexity in network systems, their interactions, and vulnerabilities to cascading effects
- Identifying gaps and shortfalls in R&D
- Creating a scientific basis for information assurance

- Developing engineering principles, practices, and evaluation benchmarks and tools
- Developing concepts for high-confidence systems and software
- Investing in information assurance for new and emerging information technologies
- Addressing the people, the process, and the legal dimensions of information assurance, including risk management (e.g., insider threat) and security process implementation

The I3P will not be a technology development "skunkworks." Its mission should encompass technology transfer, information sharing, and proactive interactions with related activities as outlined below.

Public-private information sharing

Information developed through ongoing activities is not always shared effectively either within or among sectors. But information sharing is a critically important enabler of the I3P's functions; thus, substantial care must be taken to create an effective framework. The I3P should—

- Help coordinate across sectors to ensure that information is being shared, to highlight system-of-systems interdependencies and cascading effects, and to point out where R&D and other corrective actions are required.
- Provide a neutral forum through such means as e-mail lists, web pages, chat rooms, conferences and publications (managed by I3P staff) for experts to exchange views on subjects--whether vulnerabilities, strategies, best practices, or policy--that bear on the R&D agenda for information assurance.
- Ensure that its products, including vulnerability assessments, technology, and concepts, are readily available to industry, academia, and government.

Most of the I3P's work would be publicly available; however, some necessarily would be controlled within an information management regime capable of protecting classified and proprietary information.

Day-to-day operational information sharing relating to computer intrusion, attack, or responses would not be encompassed in the organization's responsibilities, because other organizations already perform this function.

Product and services evaluation

The I3P should work with the many bodies that establish and oversee evaluation criteria and practices for evaluating new and deployed products and systems, professionals and professional services organizations, and educational programs. This work would have two goals. One would be to improve and harmonize the processes and criteria used across information technology specialties and infrastructure sectors by, for example, promulgating the best practices it observes. The second goal would be to identify research needs so that appropriate R&D can be conducted and the results fielded to raise the level of best practices everywhere. In particular, the products of the I3P's R&D program should support activities that are seeking to strengthen the evaluation of products and services, such as the National Information Infrastructure Partnership. Achieving these goals will require that the I3P be seen as autonomous, neutral and open minded by industry, academia and government.

Education and training

The execution of the R&D program should be designed to support national efforts to expand the talent pool of individuals who understand and can correct information infrastructure vulnerabilities. The shortage of such expertise is commonly cited as a significant roadblock to progress in this area. One vehicle will be sustained long-term research funding for University Centers of Excellence and other university research centers that teach information assurance. In addition, in fulfilling the responsibilities under product and services evaluation, the I3P would interact with bodies that establish and oversee educational curricula. In the course of these interactions, the I3P would make available relevant research results and materials to help build courses and training programs. Finally, the I3P's charter should permit it to support collaborative assessments and policy studies in this area.

CONCEPT OF OPERATIONS FOR THE INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION (I3P)

The concept of operations of the proposed I3P (more fully described in chapter 11 of this paper) includes the following elements:

- The I3P should be a not-for-profit organization, located in and governed by the private sector. As a private entity, the I3P would not be constrained by government pay and personnel policies and thus better able to attract needed

talent. It would not be overly burdened by government budgeting and procurement policies and thus could respond flexibly in the dynamic information technology environment. Perhaps most importantly, companies are extremely wary of sharing information with the government, suspecting it may lead to regulatory interference or public disclosure, but a properly structured I3P located in the private sector can effectively facilitate information sharing.

- The PCAST's proposal of government funding of \$100 million per year is appropriate for the I3P after an initial start up period. In addition, it may receive government funding to perform specific tasks. It also could receive private funding, although most experts believe such funding will not be forthcoming initially.
- The I3P should have a very small in-house staff of perhaps 15 to 25 professional employees. Rather than attempting to build a large, integrated research staff, it would take the more practicable approach of contracting for the external execution of its program. The staff would be responsible for strategy, planning, resource allocation, coordination, and project management. A key role of the staff is to build external relationships across infrastructure sectors.

To encourage private sector participation, the I3P would engage influential industry leaders in leading the organization and in shaping its strategy and program:

- A board of directors would govern the I3P. The directors would include prominent Chief Executive Officers (CEOs) from the companies that operate the critical infrastructure sectors and supply information technology. Their participation is essential to engaging industry in the I3P's planning and program execution.
- The I3P CEO would be chosen by and report to the board of directors. The CEO would be responsible for allocating funds and for the successful execution of the I3P program. The CEO would be a prominent, national figure, and a respected peer of the directors, able to attract talent and to work effectively with the executive and legislative branches of government.
- Corporate-government-academic steering groups would provide liaison with infrastructure providers, hardware and software suppliers, and other research organizations. They would advise the CEO in developing the I3P's R&D agenda, and in shaping its other activities. The steering groups would include Chief Technology Officers (CTOs) and government executives who would assist in gaining support and collaboration from their organizations.

Linkages with the responsible government agencies would be established through the governance structure, ongoing working relationships, and the sponsoring office:

- Some of the I3P's directors would be drawn from the National Information Assurance Council, which will include senior executives and experts appointed to advise the President on broad strategies and program priorities.
- The I3P's charter would permit it to accept tasks and funding from government agencies for specific study efforts in support of government strategy, planning, and coordination efforts in the infrastructure protection area.
- The I3P would receive its government funding and liaison support from a sponsoring organization in the Executive Branch. Preferably the sponsor would be located in the Executive Office of the President in order to emphasize its inter-agency character, but the sponsor might also be within a related government R&D activity. Other Executive Branch entities, as well as private firms, could provide additional funding for specified I3P activities.
- An interagency oversight and coordination council would review the I3P's budget and broad programmatic priorities. The council also would be responsible for promoting effective working relationships between the I3P and relevant government agencies. The council would include representatives from the National Security Council, the Office of Science and Technology Policy, the Commerce Department, the Defense Department, the National Science Foundation, and other agencies with responsibilities for infrastructure protection.

This concept of operations for I3P builds on the PCAST's original proposal and the ideas and concerns shared by experts in infrastructure protection and information assurance. This concept is best viewed as a starting point for developing a more detailed implementation approach. Specific implementation proposals should be evaluated in terms of their ability to carry out the mission and necessary functions identified here.

INTRODUCTION

The United States is highly dependent on certain basic service sectors that comprise the nation's economic and social infrastructures. Every business, industrial facility, and household operates within a decentralized, but interconnected, economic system that provides information and communications services; gas, oil, and electric energy; transportation; banking and financial services; and safe water supply, public services, and a modern public health system.¹ In 1997, after a yearlong review, the President's Commission on Critical Infrastructure Protection found that:

Certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security.... The threat of infrastructure attacks therefore has the potential for strategic damage to the United States.²

Since the Commission's report, government, industry, and academia have shown increased awareness, concern, and action regarding infrastructure protection. Many experts believe that, despite the steps taken thus far, the vulnerabilities in the nation's infrastructures are still growing more rapidly than our efforts to address them, and that much more needs to be done.

This paper assesses one important recent proposal. In December 1998, the President's Committee of Advisors on Science and Technology (PCAST) recommended establishing a Laboratory for National Information Infrastructure Protection (LNIIP) to perform research and related functions in support of critical information infrastructure protection. The proposal focused on R&D and related functions that the PCAST believes are not performed adequately today. Our assessment of the PCAST's proposal provides an independent survey of the functions needed for information infrastructure protection, and an assessment of the adequacy of ongoing activities. Our review concludes that there

¹ These are the infrastructures identified in PDD-63 and differ only slightly from those considered by the PCCIP. See *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, Executive Office of the President, May 1998.

² President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, 1997, 3, 24.

is a need for a new organization along the lines of the LNIIP to perform at least some of the proposed functions.

This study was commissioned in support of a broader government review led by the Office of Science and Technology Policy (OSTP). In February 1999, when the President responded to the PCAST proposal, he directed his OSTP staff to address three key questions.³

- Is there an existing research and development facility, either inside or outside the federal government, that might already be able to take on this function?
- Do researchers and members of industry in the private sector also see a need for such an organization, and what are their concerns and recommendations?
- Should it become apparent that the creation of the LNIIP is the best alternative, how would the laboratory function, how might it recruit (or train) the necessary talent, and how would its work complement and coordinate with research and development efforts elsewhere in the public and private sectors?

These questions have provided the broad organizing framework for IDA's review. The review was conducted in two phases.⁴ In Phase 1, IDA sought to identify those research-related requirements for critical information infrastructure protection that were not being met. Based on extensive consultation with experts in industry, academia, and government, IDA identified four functional areas requiring greater effort:

- Executing and deploying research and development
- Establishing a two-way street for public-private information sharing
- Providing product and services evaluation benchmarks and tools
- Supporting the education and training of an information assurance community

³ The letter from President Clinton was addressed to Mr. Norman R. Augustine, Chairman, Security Panel, President's Committee of Advisors on Science and Technology (PCAST), February 22, 1999.

⁴ In May 1999, the Deputy Under Secretary of Defense for Science and Technology tasked the Institute for Defense Analyses (IDA) to develop and analyze organizational options for improving public-private cooperation. The primary objectives for IDA's study are (1) to determine the scope and quality of ongoing research and development efforts in the public and private sectors (including academia); (2) to identify those areas where technical capabilities need to be improved and the best methods for doing so; (3) to develop a set of organizational options for coordinating public-private efforts to stimulate the R&D necessary to secure the critical information infrastructure in the future; and (4) to evaluate alternative organizational models to determine which one would best facilitate effective cooperation across all sectors.

An overarching finding was that the new organization must be able to shape a national agenda and broadly integrate across sectors and functions. It must motivate strong and balanced public and private participation. Overall success will be measured by how well these essential crosscutting functions are accomplished.

Phase 2 of the study refined the definitions of the four functions and considered how they might be performed. The review team augmented the findings of Phase 1 with assessments of the current state of understanding of vulnerabilities and a review of the existing activities and gaps within each of the four functional areas. Following this, the team explored several organizational structures, including the potential for performing the functions in a new organization versus assigning them to existing organizations. We developed a tentative concept of operations for the proposed new organization.

Our assessments and findings are presented as follows. Part I outlines the context for this study and summarizes the views of the experts interviewed. Chapter 1 provides a brief overview of the PCAST's proposal. Chapter 2 presents the experts' assessments of the PCAST proposal as well as their perspectives on related information infrastructure issues.

Part II presents our assessment of the current state of knowledge regarding infrastructure vulnerabilities, as available in unclassified form. Chapter 3 begins with a look at information system and network issues common across infrastructures. Chapter 4 focuses in greater depth on specific sectors.

Part III summarizes our examination of each of the four functional areas. The purpose of this work is to clarify needs in each area and to assess the adequacy of current activities. Chapter 5 provides an overview of our approach and identifies the activities that are reviewed. These represent our baseline for determining what new initiatives might be needed. The following four chapters then focus on each of the four functional areas: research and development (Chapter 6), information sharing (Chapter 7), product and service evaluation methods and tools (Chapter 8), and education and training (Chapter 9).

Part IV evaluates the case for establishing a new organization to perform the needed functions identified in Part III. Four broad alternatives, including their potential

strengths and weaknesses, are outlined in Chapter 10. Chapter 11 then outlines a concept of operations for the proposed Institute. Appendixes provide additional supporting materials.

PART I
THE EXPERTS' VIEWS ON THE PCAST PROPOSAL

Chapter 1

BACKGROUND: THE PCAST PROPOSAL

In May 1998, the President responded to the recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP), issuing Presidential Decision Directive 63 (PDD-63). The directive expressed the President's intent that the critical infrastructures, and especially the underlying cyber systems, be protected from significant vulnerabilities to physical and cyber attacks.¹ The document called for a public-private partnership and defined a liaison structure matching lead federal agencies with private sector counterparts in each infrastructure sector. It called for a National Infrastructure Assurance Council to ensure high-level federal contact with major infrastructure owners and state and local government officials. It proposed that each economic sector create an information sharing and analysis center (ISAC) and designated certain agencies to serve as liaisons with key infrastructure sectors. PDD-63 also established mechanisms for interagency coordination at the federal level. Individual agencies were responsible for developing plans for protecting the federal infrastructures, with OSTP providing overall oversight and coordinating government research and development activities.

In a letter to President Clinton on December 10, 1998, the President's Committee of Advisors on Science and Technology (PCAST) proposed an additional step: the establishment of a new organization to generate and disseminate knowledge related specifically to the cyber vulnerabilities of the nation's critical infrastructures.² This Laboratory for National Information Infrastructure Protection (LNIIP) would be a research and development center and would perform various functions related to information infrastructure protection but would not be involved in operations or implementation. The LNIIP would be a federally funded, not-for-profit organization with private sector advisors and support.

¹ See *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, Executive Office of the President, May 1998, 1.

² The PCAST's letter to President Clinton (December 10, 1998) is included in Appendix A.

The purpose of the new organization would be to conduct research and develop technology to protect critical information and communication systems from penetration or damage by hostile foreign groups, organized crime, and determined hackers. The organization would also address protection of these complex, nonlinear networks from major disruptions due to natural instabilities, internal design weaknesses, and human failings.

The PCAST identified a number of tasks for the LNIIP to pursue:

- Gain a systematic understanding of information infrastructure vulnerabilities. Develop a broad understanding of the robustness and resilience of such complex systems, and create the means to assure graceful degradation under stress.
- Conduct research and develop technology to protect the critical information and communication systems. Develop and deploy new technology equipment, software, and procedures.
- Provide a linkage among government, industry, and academia to serve as a clearinghouse for industry information and experience; set and disseminate best practice information; and carry out training exercises and inspections to certify performance.

The proposed organizational structure for the LNIIP is depicted in Figure I-1. An independent board of directors composed of leaders from the information technology supplier and customer industries and from academia would govern LNIIP. A Federal Coordinating Committee, acting for an interagency National Information Infrastructure Council, would provide government oversight. Federal funding, which might grow to \$100 million, would be provided through the Office of Management and Budget (OMB). An industry advisory committee would also provide external oversight. The LNIIP would serve clients in the government and the private sector and would eventually generate financial support from the latter.

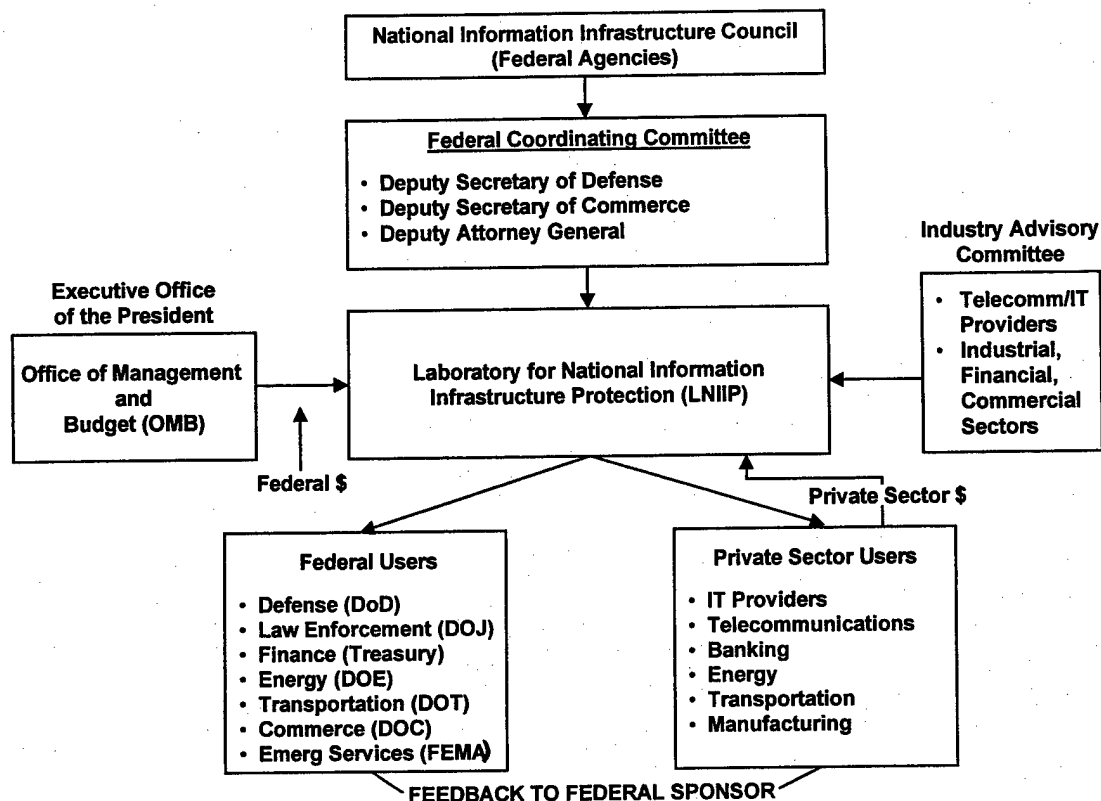


Figure 1-1. PCAST's Proposed Organization

A Federal Coordinating Committee would define the LNII's research requirements. The LNII would interact with federal and private sector users to give them a role in shaping the work program. The technical program would focus on the following topics:

- Vulnerability detection and analysis
- Security architectures and simulation systems
- Encryption and authentication systems
- Intrusion detection and warning systems
- System recovery
- Component and software security assurance
- Best practices for product evaluation
- Training
- Human interface with complex systems

The PCAST-proposed LNIIP provided the starting point and focus for the IDA review. As explained in the subsequent chapters, the review considered modifications to the PCAST model, as well as substantially different structural alternatives.

Chapter 2

THE EXPERTS' VIEWS ON THE PCAST PROPOSAL

Between May and September 1999, the IDA study team interviewed representatives of industry, government, and academia, including members of the policy community and the PCAST, to gather their views concerning the PCAST proposal and related issues.¹ The interviews focused on the questions posed in the President's February 1999 response to the PCAST proposal and related issues.² The IDA study team supplemented the interviews with workshops in June and September. These provided opportunities for experts to discuss the PCAST proposal and to suggest other approaches. In addition, IDA drew on a White House conference that included the President's Science Advisor, the National Coordinator for Critical Infrastructure Protection and Counterterrorism, PCAST members, and the Chief Technology Officers from fifteen major information technology firms.

In summarizing the results of these activities, we have grouped the experts into three broad categories, roughly corresponding to industry, academia, and government. The industry representatives include information technology (IT) vendors (namely, software and hardware developers and manufacturers), infrastructure operators (including utilities, telecommunications companies, and internet service providers), and end users

¹ In all, more than 100 experts contributed to this study. A list of interviewees and workshop participants can be found in Appendix B.

² The IDA interviewers posed five questions:

- What organizations and programs are currently addressing the problem of information infrastructure protection, and how effective are they?
- What are the major gaps and limitations in existing research and development programs, approaches to developing and deploying new technologies, and education and training? What factors contribute to these deficiencies?
- What is the appropriate role of government in finding or facilitating fixes for these deficiencies? What role should industry and academia play?
- Is a Laboratory for National Information Infrastructure Protection the right approach?
- What other organizational models might better serve the goal of enhancing the security of the nation's information infrastructure?

(such as insurance companies and defense manufacturers). The academic category includes both university faculty and researchers in private think tanks. Government interviewees include representatives of the Department of Defense (military and civilian), civilian agencies, national labs, and Congress. In a few cases, interviewees span categories—as in the case of former government officials now employed in think tanks, universities, or business—and their responses are occasionally divided between categories depending on which community they were speaking for when they expressed their views on a given issue.

A. NATURE OF THE CHALLENGE

Experts share the conviction that vulnerabilities in the nation's information infrastructure pose a danger to both the national security and the economic health of the nation. Current views reflect a dramatic increase in the level of understanding and awareness of infrastructure vulnerabilities in recent years. The experts characterize the fundamental underlying problem as stemming from the rapid decentralized growth in networked information systems. No one fully understands the behavior of the networks that have been created, the interactions among them, or how they interact with the physical systems they control. At the same time, there has been too little emphasis on establishing the design principles and engineering tools for building networks that incorporate robustness, assurance, and security. In subsequent chapters, we will survey current assessments of vulnerabilities.

In examining possible initiatives to address vulnerabilities in today's complex information networks, the experts see major challenges in defining responsibilities and working relationships among government, industry, and academia. Gaps in research exist today because existing competitive mechanisms (in both commercial markets and research communities) typically do not fund long-term research or research on the kinds of broad systems-of-systems issues that often give rise to vulnerabilities. There are important crosscutting issues that are too broad and too complex for industry or academia alone to tackle.

There is wide agreement, therefore, that the government should play a leading role in any coordinated national response to these vulnerabilities as a function of its obligation to protect the national security of the nation. In particular, the government has responsibility to improve the understanding and awareness of vulnerabilities and the crucial links between improved information assurance and national defense. At the same

time, an effective R&D program will require active industry involvement, and industry must take the lead in addressing the vulnerabilities identified.

There are major barriers to establishing cooperative relationships, not just between government and industry—which is in itself daunting—but within industry, which could prove as difficult, if not more so. Cooperation has been problematic in the intensely competitive business environment. In addition, legislators need to address the statutory restrictions current anti-trust laws place on industry cooperation.

Fortunately, the business community has, over the past few years, come increasingly to recognize the potentially catastrophic costs related to information infrastructure vulnerabilities. The level of private sector energy and resources devoted to information assurance is increasing (one source reported the information assurance market has grown fourfold between 1996 and 1999), and industry collaboration—both internally or with government and universities—is beginning to take hold (particularly in the banking and financial sectors).

These developments suggest the time is right for engaging industry in a collaborative effort. Corporate executives caution, however, that progress will require careful consideration of the equities of all the parties involved and focused efforts to transcend cultural boundaries and eliminate legal boundaries to cooperation. Currently, government, industry, and the academic communities (and sub-groups within each of those communities) view information infrastructure vulnerability from different perspectives, and as a result, each tends to conclude that the others do not fully understand the severity and complexity of the challenge.

We found agreement on two additional issues regarding the scope and nature of the problem: 1) that infrastructure vulnerabilities pose a multidimensional problem that demands creative and interdisciplinary approaches extending beyond software and hardware engineering to basic science, sociology, ethics, and law; and 2) that the constant evolution of information technology makes efforts to address such vulnerabilities a rapidly moving target, or more accurately a set of targets that will continue to defy permanent or one-size-fits-all solutions. These two insights constitute fundamental principles that, combined with the awareness that the nation's security depends on the establishment of a secure information infrastructure, should underlie any attempt to craft an institutional response to the challenge of protecting the national information infrastructure.

B. WHAT IS TO BE DONE?

The experts support creation of an organization that would map out key networked information systems, explore the behavior and vulnerabilities of such complex systems-of-systems, and develop technologies and methods for addressing vulnerabilities. They identified a number of research areas where gaps and limitations in current understanding need to be addressed. The functional areas that are not adequately covered by existing organizations or programs fall into four areas:

1. Executing research and development and fielding the results
2. Establishing a two-way street for public-private information sharing
3. Fostering improved evaluation of product and services
4. Supporting the education and training of a pool of information assurance professionals

We examine each of these four functional areas in detail in Part III of this report.

Beyond these specific functions, the experts believe that the core mission of any new organization should be to help formulate a national strategy that integrates effort across economic sectors and among the public, private, and academic research communities and places heavy emphasis on the dissemination application of new knowledge. While a great deal of work is ongoing in the information assurance area—in government, industry, and academia—the mechanisms for integrating and fielding new breakthroughs remain inadequate. As one interviewee noted, the state of the nation's information assurance could advance dramatically if only we were to get what researchers and engineers already know into the marketplace.

Many of the experts we consulted stressed the need to integrate activities. They noted that federal efforts in this realm have yet to gain the confidence and support—and sometimes even the attention—of industry. Executives believe federal responses thus far have been poorly coordinated and underfunded, suffering overall from the absence of a coherent national strategy. Executives also see a lack of a concrete commitment at the highest level of government backed by the kind of long-term funding allocations that would indicate that the federal government is serious about tackling the problem over the very long-term. Numerous organizations within government are currently addressing some aspect of the information assurance problem, but outside government (and, to some extent, even within government) these efforts are perceived as marginally effective, at best. They lack a single, highly placed advocate to provide focus and interface with the

private sector. In short, until someone in government "owns" responsibility for integrating public and private approaches to addressing the problem of information assurance and fostering concrete and effective responses, industry is unlikely to recognize that not just their bottom-line but the overall security of the nation is at stake.

C. IS A LABORATORY THE BEST ORGANIZATIONAL APPROACH?

At the conclusion of our Phase 1 review, it was clear that the level of understanding and concern among experts about information infrastructure vulnerabilities has expanded significantly in the last 3 years. It was equally clear that there is support for some level of government action to jump-start the important new functions that need to be performed. There was, however, no consensus on whether the creation of a new organization would be helpful in performing the needed functions. The experts offered widely ranging views on possible alternatives to the PCAST-proposed laboratory. Some contended that a new organization is not needed and that expanding the programs of existing is enough to fulfill the needed functions. Others favored assigning those functions to a new government agency. There was also support for attempting to create an industry consortium to perform these responsibilities.

Those who supported the PCAST's laboratory model cited a number of key research areas that need the kind of unbiased attention that a government-sponsored laboratory is most likely to give. In some crucial areas, such as understanding networked information systems as end-to-end systems-of-systems, there was a sense that only a dedicated laboratory could devote the attention and resources necessary to see complex research problems through over the long term. Several interviewees also cited important work already underway at Department of Energy Labs (Livermore, Sandia) as examples of the kind of work that can be done only in such an environment. Proponents raised several additional considerations that might make a laboratory desirable. These include the need to establish an evaluation capability, such as that provided by Underwriters Laboratories, for information assurance; the government's unique qualifications as an "honest broker" and facilitator of information sharing; its long experience dealing with classified and sensitive information; and its already sophisticated threat assessment capabilities.

Interviewees who disagreed with the PCAST proposal often objected specifically to the notion of its being a "laboratory." To them, this connoted the creation of a new facility and building and a large onsite staff of information technology experts.

Opponents and skeptics cited several potential obstacles to establishing such a laboratory from scratch: (1) the high start-up costs, (2) the shortage of qualified talent (which creation of a laboratory could make even worse), (3) the likely inability of a government laboratory to compete with the private sector for qualified personnel, (4) industry's likely reluctance to share proprietary information, (5) various cultural and organizational impediments to effective public-private cooperation (including Freedom of Information Act concerns, copyrights, licensing, and other intellectual property concerns), (6) the risk that a new organization would drain resources (especially government R&D funding) from ongoing efforts, and (7) the feeling that a laboratory would focus efforts inappropriately. The challenge is not so much doing new research as coordinating, disseminating, and putting to use the research that is already being done in industry, universities, and existing government laboratories.

Academics and industry representatives often expressed the view that government laboratories have, in the past, tended to become divorced from the academic and business mainstream and have a poor record of commercializing the technologies they develop. Industry representatives voiced further concern that "mission creep" might ultimately lead a new government laboratory to become (or at least appear to be) an economic competitor to the IT industry. In addition, there was a general sense that bureaucracy, funding problems, interference from the intelligence and law enforcement communities, and flagging interest once it appeared that government systems were secure would hobble any new government organization. As a result, almost everyone interviewed said that any new organization should be established outside government with carefully structured functions so that industry sees it as a partner rather than as a potential economic competitor.

D. IF NOT A LABORATORY, THEN WHAT KIND OF ORGANIZATION?

Although there was considerable resistance to the idea of a new government laboratory, we found that the experts agreed with the PCAST on both the need for greater coordination between public and private efforts to ensure the security of the nation's information infrastructure as well as on the basic functions that need to be performed. The debate over alternative organizational approaches focused on questions of what kind of organization will best meet those needs. The negative reaction to the idea of a laboratory focused on a few key issues. A few, subtle modifications—increased emphasis on industry leadership and involvement, an R&D agenda focused tightly on areas currently not addressed by industry or government, and limiting the new organization to a

small in-house staff combined with a strong external program—yielded a version of the PCAST proposal that found considerable support. This report evaluates this modified PCAST model—what this report refers to as the I3P (Institute for Information Infrastructure Protection)—instead of the “laboratory” model.

Several other models were also suggested and discussed by the experts. In Chapter 10 we define and evaluate four broad structural alternatives that represent the range of ideas presented in our interviews and workshops. The four alternatives evaluated are:

- The I3P, as described above (government-funded, private organization)
- a programmatic initiative that would expand funding for current efforts within existing organizations
- a new, mission-focused government agency or office, and
- a purely private sector consortium.

The experts emphasized that creating a new organization will help only if it represents a demonstrable improvement over existing organizations—after all, a program initiative funding additional work within existing organizations is the most straightforward approach. In addition, a new research organization that is one among many peers in this area will not accomplish the needed coordination and integration. Taking a leadership role, a new organization would need to help forge a national strategy for protecting the nation’s information infrastructure, integrate across the existing activities, and accelerate industry’s application of new technologies and practices.

Chapter 10 evaluates each of the four structural alternatives using these and other specific evaluation criteria. This detailed assessment concludes that the PCAST’s proposal, as modified to form the I3P, is the approach that best reflects the characteristics identified by the experts in our interviews and workshops. These are summarized in the following paragraphs.

1. A Strong Private-Sector Role

Most experts advise that the key challenge in information infrastructure protection is to engage firms to share information and collaborate among themselves as well as with the universities and the government. To accomplish this, the new organization should be a not-for-profit private organization with a board of directors drawn from industry (and including vendors, infrastructure operators, and end-users) along with direct and regular

access to national leaders, including the President, Departmental Secretaries, and responsible members of Congress.

Companies are wary of sharing information with the government, suspecting it may lead to regulatory interference, law enforcement intrusion, or public disclosure. A properly structured organization located in the private sector could effectively facilitate information sharing. Moreover, a private-sector organization would not be constrained by government pay and personnel policies and would be better able to attract needed talent. It would not be overly burdened by government budgeting and procurement policies and thus could respond flexibly in the dynamic information technology environment.

2. Strong Leadership, Lean Staffing, and Strategic External Relations

An effective and influential organization would have the following key attributes:

- A director of sufficient stature and charisma to attract the best and brightest talent, engage support and participation of key corporate CEOs, and wield sufficient influence with both the executive branch and Congress. Likewise, the organization's Board members should be individuals widely known for their vision and political sophistication.
- A small permanent staff augmented by a larger staff of information assurance experts and engineers who rotate in from industry, academia, and government. Such a rotating staff serves two purposes—it keeps the institution tied to the outside world and ensures that its research program will keep up with the rapid pace of technological change.
- A business model that is compatible with that of the information technology industry. The IT industry is culturally quite different from the heavy industries (aerospace, automotive, chemical) that previously have been the prime government contractors, accustomed to security and accounting requirements. In particular, the a new organization would need to be empowered (probably by statute) to operate outside standard (and cumbersome) government contracting and auditing procedures and mechanisms would need to be established to address industry concerns over intellectual property rights.
- A physical or virtual connection with one or more high-tech centers (Silicon Valley, Austin, Chicago, Northern Virginia, or Boston). Some experts suggested that a "virtual laboratory" linking academic and industry research facilities would be adequate. Others, however, held that the establishment of a physical center in close proximity to industry and academic centers of excellence would probably be necessary.

3. Stimulating Research Environment

A core of smart people working on inherently interesting problems combined with an exciting and innovative research agenda will attract interest and talent. Early breakthroughs, however limited, could also attract new talent.

4. Direct Partnership with Industry

The governing structure of any new organization must be truly public-private, with "captains of industry" sitting on the Board of Directors and committed to supporting its information protection mission over the long term. The partnership must be proactive and spur real public-private-academic cooperation rather than merely bringing existing activities under a single administrative and funding umbrella.

5. Committed, High-Level Government Sponsorship

There was agreement that any new organization would require a strong partnership with the government. The sponsoring agency would need the institutional clout to protect the organization's interests in the interagency process as well as with Congress, some experience in managing long-term R&D programs, and a strong commitment to the mission. The Executive Office of the President, the Department of Defense, and the Department of Commerce were most often mentioned as the logical sponsors of such an organization.

A majority of the experts we interviewed agreed that the Department of Defense has the best record of overseeing managed research and development and technology transfer and has the institutional clout to defend the new organization and its mission in the interagency process and promote its interests in Congress. There were strong concerns, however, especially among industry representatives and university researchers, that the research agenda of an organization associated with DoD would be captive to military and intelligence collection priorities of its sponsor rather than broader private sector vulnerabilities. DARPA was often mentioned as the Defense agency best suited to sponsor the new organization, but many interviewees deemed it too small and too focused on development. Some argued that DARPA is not set up to oversee long-term research (over 5 years). And, some noted, DARPA would inherit most of the defense baggage that might undermine DoD as a sponsor without the balancing advantage of the larger agency's clout.

Interviewees in all three sectors conceded that the intelligence community has by far the best grasp of the scope and nature of likely threats, as well as big budgets and a huge head start in mastering the technical problems involved in protecting the information network from hostile attacks. But industry and academia also view the intelligence community with a great degree of suspicion and thus do not regard it as an appropriate institutional home for the overall mission—although its participation would be important and, at any rate, inevitable. In fact, private sector representatives go so far as to suggest that industry is unlikely to cooperate with any initiative concerning standards, research and development, or information sharing in which the intelligence community and law enforcement plays a central or visible role.

A significant number of interviewees mentioned the Department of Commerce as the logical sponsor for such an organization. It is the federal agency with the closest working relationship and cultural empathy with industry and business as well as with the relevant congressional appropriation and oversight committees. It is also the current home of the Critical Infrastructure Assurance Office (CIAO) and, under the critical infrastructure protection structure defined in PDD-63, the lead agency for liaison with the information and communications sector. Still, most of those interviewed (including those who supported Commerce as the sponsoring agency) believe it lacks two critical success factors: the interagency clout to ensure the success of the new organization and experience in working closely with industry in long-term R&D and technology transfer. Moreover, the ongoing information infrastructure protection efforts within the Department of Commerce are thus far unproven in the eyes of industry. A few interviewees also expressed concern that industry and academics might deem the Department of Commerce too close to the intelligence community.

6. Adequate and Secure Funding

Industry, government, and academia disagree most dramatically over who should pay for research in the private and academic sectors. Experts from industry and academia often contend that information assurance is a national security matter for which the government should fund relevant R&D just as it funds R&D relevant to military defense. But even if the government provides the bulk of the necessary funding, most industry representatives see it primarily as a coordinator of any new organization's R&D efforts and warn that government should not seek to control the research agenda or its implementation if it expects industry cooperation. Representatives of government, in

contrast, generally hold that information assurance is essential to the functioning of business and therefore the private sector should provide a significant share of the human *and* financial resources necessary to tackle the problem. In short, while both sides agree that ideally government and industry should cooperate in addressing information infrastructure protection, each thinks the other should provide more funding than it now does.

Almost all experts agree, however, that initial funding will have to come primarily from government. Any new organization must first build a portfolio of impressive deliverables in order to prove to industry that any future investment will bring real payoffs. Industry will want government to "put its money where its mouth is." Moral suasion is not enough—only by putting dollars to work on the problem can government convince industry of its commitment. After the new organization has proved its mettle, greater financial commitment from business might be possible (but should not be counted on in the near term).

The experts' views summarized in this chapter have focused on the information assurance problem at a broad, conceptual level. While there are widely divergent views among the experts, three general conclusions summarize the current state of thinking. First, the level of awareness and concern has grown significantly in the past couple of years. Experts in government, industry, and academia now agree that infrastructure vulnerabilities pose a significant risk that must be addressed on several levels – to individual businesses, to collective industries and sectors, and to US national and economic security. Second, several functions need to be expanded and strengthened in order to better understand and address vulnerabilities. Third, a new organization would strengthen these functions if it were structured to engage industry, academia, and government in forging an integrated, national approach. Of critical concern is the need to engage industry participants in designing and executing the functions.

The analyses and assessments in the following chapters provide a detailed description of the state of understanding of information infrastructure vulnerabilities, the functions that need to be strengthened, and an explanation of why the I3P presents the best approach for addressing these needs. In the final chapter, we draw this work together in the form of a proposed concept of operations for the I3P.

Part II

Growing Awareness of Infrastructure Vulnerabilities

Chapter 3

GAINING AN UNDERSTANDING OF CYBER VULNERABILITIES

It is now widely accepted that networked information systems are vulnerable to cyber attack and that hostile actors are exploring how they might take advantage of that vulnerability. No one understands the vulnerabilities with sufficient clarity, however, to identify all the steps necessary to protect the critical information infrastructure. In particular, not enough is known to build a business case for more private research. Because the potential risk is of strategic importance for the U.S., it is essential that this gap in understanding be closed.

In this chapter and the one that follows, we review several current unclassified assessments of current vulnerabilities. The goal is to establish a clearer view of the kinds of research needed to understand and address vulnerabilities, and to identify where the gaps are in current research and development programs. In this chapter we consider the generic vulnerabilities associated with the ways business is employing networked information systems. In the next chapter, we examine several sectors in more depth in order to illustrate some of the ways in which vulnerabilities depend on the specific applications of networked information systems by each sector.

A. BACKGROUND

In its 1997 report, the PCIIP noted that the United States was only beginning to understand its vulnerabilities.¹ It nevertheless concluded that the risk to the United States was sufficient to require federal action:

The threat of infrastructure attacks therefore has the potential for strategic damage to the United States. Accordingly, the assurance of critical infrastructures deserves national attention and leadership by the federal government. ... Protecting our infrastructures into the 21st century requires

¹ See President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, 1997, 5, 6.

that we develop greater understanding of their vulnerabilities and act decisively to reduce them.²

Another government report, *Cybernation*, similarly emphasized the need for careful study of the vulnerabilities of the critical infrastructure sectors. It noted that the United States must develop "a sense of proportion about threats and vulnerabilities" through an "analytical understanding of the specific reliability, vulnerability, and threat environment" based on a "systematic sector-by-sector analysis." Further, the paper notes that "many of the recognized threats to the information networks supporting the domestic infrastructure have not actually been experienced."³

This is fortunate, but it also means that experience to date has not fully disclosed the targeted vulnerabilities and exploitation methods of potential attackers.⁴ Specific defenses cannot be devised unless the vulnerabilities are better understood.

Another observer notes that the United States lacks the experience to understand strategic cyber attacks, i.e., concentrated, sustained, and simultaneous attacks at multiple points.⁵ We have neither the experience to gauge the consequences of national-level cyber attacks nor the ability to assess the level of effort that would be required to execute such attacks or their probability of success.

To understand the vulnerabilities and risks associated with the dependence of critical infrastructure sectors on networked information systems, a wide information gap must be closed.⁶ The first-order research questions include at least the following:

- What is the structure of the nation's key networked information systems, and how are they interconnected?

² Ibid., 6, 24.

³ See *Cybernation: The American Infrastructure in the Information Age, A Technical Primer on Risks and Reliability*, Executive Office of the President, 1997, 2, 3, 5, 7.

⁴ Of course, the Internet is replete with information on the vulnerabilities of general information networks and exploitation methods. At issue here is information specific to deployed networks in particular sectors.

⁵ See Stephen J. Lukasik, "Protecting Information-Dependent Infrastructures," *Information Impacts Magazine*, <http://www.cisp.org/imp/>, September 1999, 4.

⁶ Risk is viewed here as a measure of expected loss in terms of national or economic security. Risk depends on the infrastructure vulnerabilities, the threats that would exploit those vulnerabilities, and the consequences of exploitation.

- What are the systemic vulnerabilities in these structures that could be exploited? To what extent are vulnerabilities unique to individual sectors versus common to two or more sectors?
- How seriously could a cyber attack damage each of the infrastructure sectors, i.e., what would be the extent of the damage, the recovery time, and the recovery costs? How would potential damage scenarios affect military effectiveness, public confidence and safety, and national policy? How long could attacks continue before each of the infrastructure sectors could be made secure or attackers could be neutralized?
- What must an adversary do to prepare an attack that would cause serious damage, e.g., what information is required and who has sufficient organizational capability to mount a major attack?

Some of the work that is beginning to address these questions is surveyed in the remainder of this chapter. We describe some of the general concerns arising from the growing use of networked information systems and automatic control systems, and then assess what is known today about the capabilities of potential attackers and actual attacks that have been perpetrated.

B. INFRASTRUCTURE VULNERABILITIES AND NETWORKED INFORMATION SYSTEMS

Dependence on critical infrastructure sectors is not new. What is new is that the sectors have become more dependent on networked information systems for operations as well as business management. As operational control systems and other critical functions have been automated, infrastructure services have become subject to the vulnerabilities of complex computer and communications networks.

The automation and centralization of core infrastructure functions have magnified the potential consequences of a well-informed information infrastructure attack. Whoever controls the control system controls the infrastructure to a frightening degree. A disgruntled insider could potentially shut the infrastructure down. The leverage of automated controls may also be available to knowledgeable outsiders if they can access them through remote-access facilities.

Moreover, individual organizations are increasingly interconnecting their networks, internally and externally, via both dedicated channels and the Internet. Market forces and information technology are driving companies to closer business and operational relationships. Electronic commerce is linking operators with suppliers,

customers, and peers. In sectors such as energy and telecommunications, deregulation has greatly increased the number of organizations jointly involved in providing services, again increasing the number of required interconnections. This raises the risk that malicious outsiders could exploit such linkages to penetrate critical internal systems, either directly or via other systems connected to critical systems. Further, greater interdependence raises the likelihood that disruptions of one network will cause cascading disruptions both within and between infrastructure sectors. Each network potentially takes on the vulnerabilities of all the networks to which it is connected.⁷

While mission-critical systems nearly always reside on dedicated networks, increasingly, such networks are being connected to other networks that have external connections via the Internet or modem. This provides a vulnerable point of access that potentially exposes mission-critical systems to anonymous attacks from throughout the world.

In sum, the dependence of critical infrastructure sectors on networked information systems raises new issues about their trustworthiness.⁸ The potential for accidental or deliberately induced failures and misuse of these systems poses a risk for those who depend on the infrastructure sectors. Service may become unavailable or unreliable, and information may be stolen or corrupted.

C. VULNERABILITY OF AUTOMATED CONTROL SYSTEMS

Critical infrastructure sectors can be disrupted by the failure or misuse of their automated control systems.⁹ These systems are complex networks of disparate components, subsystems, and communications links that are substantially controlled by software. Systems may fail in a discrete way if key components fail, for example, if the central computer loses power. They may also fail in a chain reaction if anomalous events ripple through tightly coupled subsystems, for example, when a downed power line leads

⁷ Organizational interfaces can be particularly vulnerable because they tend to diffuse responsibility and open the door to errors that attackers can exploit. See Lukasik, "Protecting Information-Dependent Infrastructures," 2.

⁸ For a careful discussion of trustworthiness, see National Research Council, *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, 1999, 13-20. That study defines *trustworthiness* to include correctness, reliability, security, privacy, safety, and survivability. In turn, *security* is said to encompass secrecy, confidentiality, integrity, and availability.

⁹ This section borrows heavily from *Cybernation*.

to a massive power blackout.¹⁰ Failures may occur accidentally or may be triggered by malicious misuse or attack.

Most infrastructure control networks are combinations of interconnected and interdependent networks, operating together to provide real-time control. Each system's performance depends on the unpredictable interactions of its subsystems and the full system's tolerance for component and subsystem faults. Even a complex system can be made robust, with redundancy in critical subsystems and provisions to contain cascading events. However, system designers must make tradeoffs among reliability, cost, and performance. Moreover, infrastructure control systems rarely reflect a single top-down design. Instead, they evolve over time as customer requirements expand, technologies change, and software is updated. There is a constant need to engineer solutions to problems that emerge. The susceptibility of a network to major disruptions, then, can only be judged by carefully assessing many technical factors.¹¹ Without careful study, it is not readily apparent how prone a system is to failure.

Cybernation (pp. 18–19) provides a roadmap for the study of information system vulnerabilities, identifying the following key system elements and their vulnerable points:

- Operational concept (e.g., range of computer control, scope of remote commands, options for external entry, response to failures and data corruption, recovery process)
- Architecture and information flows (subsystem interactions, tightness of subsystem coupling, system tolerance to degraded components, failure modes, provisions to contain cascading effects, redundancy, interconnection with other networks)
- Network components (operating limitations or design flaws in critical components such as supervisory control and data acquisition (SCADA) systems, gateways, firewalls, routers, servers)
- Signal protocols and transmission methods (encryption capability and susceptibility to monitoring, interception, interference, spoofing, or jamming)
- Human factors (human judgment in the loop, carelessness, inattention, procedural error, well intentioned workarounds, personnel reliability)

¹⁰ In July 1996, for example, a transmission line in Oregon sagged into trees and short-circuited, overloading and shutting down other lines, eventually including the main links to California. Safety systems shut down generators that were overwhelmed by the resulting excess power demands. Altogether, 15 states were affected. This example is recounted in *Cybernation*, 12.

¹¹ See *Cybernation*, 12.

- Existing security environment (security of password files, access to supervisory features, integrity of access logs, ability of administrator to detect intrusions, implementation of security tools)

One of the more difficult engineering challenges is ensuring the reliability of the software for infrastructure control systems.¹² Validating such complex software requires exhaustive testing, which can be prohibitively expensive and may not be technically feasible. Further, increasing reliance on outsourced software development and commercial-off-the-shelf products can leave infrastructure operators with insufficient information to understand or validate critical control software. Software updates may introduce logical and coding errors, undo previous corrections, and alter timing. Malicious code may be deliberately and surreptitiously included during software development or modification.

D. POTENTIAL THREATS

The government is concerned about the national security implications of increased infrastructure risk.¹³ Most seriously, foreign governments may execute organized attacks on our critical infrastructure sectors by exploiting their cyber vulnerabilities. George Tenet, Director of Central Intelligence, has testified:

We know with specificity of several nations that are working on developing an information warfare capability.... These countries recognize that cyber attacks—possibly launched from outside the U.S.—against civilian computer systems in the U.S. represent the kind of asymmetric option they will need. ... (T)he battle-space of the information age will surely extend to our domestic infrastructure. Our electric power grids and our telecommunications networks will be targets of the first order.¹⁴

¹² Ibid., 11–12.

¹³ The PDD-63 white paper notes that “non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.”

¹⁴ Tenet notes that several countries have government-sponsored offensive and defensive information warfare programs and that information warfare is included in their military doctrines and war college curricula, for both battlefield and civilian arenas. See George J. Tenet, “Testimony by Director of Central Intelligence George J. Tenet before the Senate Committee on Government Affairs,” June 24, 1998, 2–3. Two additional documents are also of interest: Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999); Andrew W. Hull, *The Chinese Approach to Information Warfare*, IDA Document D-2432, Institute for Defense Analyses, Alexandria, VA. Another experienced observer, however, notes that the planning of cyber

Tenet similarly notes a serious threat from sub-national groups:

Terrorists, while unlikely to mount an attack on the same scale as a nation, can still do considerable harm.¹⁵

Other potential threats include attacks by organized crime groups, malicious hackers, and disgruntled insiders. The government's concern over these latter threats may be more a matter of law enforcement or economic security than of national security *per se*.

The information warfare activities of other governments were also noted by the deputy commander of DOD's Joint Task Force on Computer Network Defense:

The odds of the U.S. being attacked on line by a foreign nation state in some kind of cyber war in the near future are probably pretty low. But the odds of foreign nation states wanting to develop capabilities to help them if and when we are adversaries are probably pretty high. We need to have the same capability or better.¹⁶

Cybernation (pp. 15-16) discusses three categories of potential attackers:

- *Computer hackers* motivated by technical challenge, mischief making, or theft will perpetrate small-scale intrusions resulting in altered or destroyed data or locally degraded operations, with the potential to trigger cascading failures inadvertently.¹⁷
- *Anarchists* motivated by malice or criminal purpose will deliberately seek to damage infrastructure sectors by attacking critical components or corrupting software and data. They will not necessarily conduct a careful assessment of the precise effects of their attacks but could easily trigger major disruptions.
- *Coordinated cyber attacks* by more sophisticated attackers motivated by strategic political goals will be organized carefully to yield specific outcomes. Techniques will include hacking, planting Trojan horses or logic bombs in operating system software, and co-opting insiders with specialized knowledge.

attacks and their integration into military doctrine are in their infancy. See Lukasik, "Protecting Information-Dependent Infrastructures," 8.

¹⁵ See Tenet, "Testimony by Director of Central Intelligence," 3. Note also that even lower-scale attacks may undermine public confidence in the information infrastructure and weaken support for the government.

¹⁶ This comment by Navy Captain Bob West was reported in Frank Wolfe, "Task Force Monitoring Cyber Intrusions around the Clock," *Defense Daily*, July 27, 1999.

¹⁷ Hackers also use tools such as trin00 and Tribe Flood Network (TFN) to launch massive denial of service attacks on particular networks by causing hundreds of compromised computers to send certain messages to the intended victim via the Internet.

The result could be major disruptions and cascading failures, although the attackers may prefer precise outcomes to unpredictable cascading effects.

Cybernation posits that the same level of damage could be achieved by attackers in any of these categories.

E. THE GROWING BODY OF EVIDENCE ON VULNERABILITIES

There is ample evidence that critical infrastructure outages result when information networks are beset by natural phenomena, component failure, or human error. There are alarming statistics on attacks by computer hackers and a number of anecdotes about hackers penetrating internal control systems. There are also anecdotes about foreign governments and sub-national groups probing or attacking U.S. networks. However, there have not been instances of hostile attacks causing severe disruptions of critical infrastructure sectors in this country.¹⁸

There are, in contrast, many examples of non-deliberate, severe disruptions of critical infrastructure sectors.¹⁹ Natural phenomena often cause outages, for example, a 1994 earthquake in Northridge, California caused an 8-hour disruption of long-distance telephone service when two major switching facilities failed. In September 1991, equipment and human failure combined to shut down half of AT&T's long-distance traffic for New York City. A power generator failed and batteries were depleted after workers ignored alarms for 6 hours. The shutdown affected 90 percent of communications with the New York air traffic control center, forcing the cancellation of flights and inconveniencing air travelers for 8 hours. Other disruptions are caused by faulty software. In August 1999, problems during a software upgrade at MCI Worldcom disrupted its high-speed frame-relay data service for 10 days, forcing the Chicago Board of Trade to shut down its electronic trading system and preventing a number of Internet service providers from serving all of their customers.²⁰

¹⁸ One study defines a severe disruption as a sustained interruption or degradation, with potential strategic and/or service integrity significance, affecting at least one region and major metropolitan area, significantly degrading at least one critical infrastructure, enduring for at least a significant portion of a business day. See President's National Security Telecommunications Advisory Committee, "Internet Report: An Examination of the NS/EP Implications of Internet Technologies," Network Group, June 1999, 2.

¹⁹ See, for example, *Cybernation*, 13-15, and National Research Council, *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, 1999, 16-20.

²⁰ See *The New York Times*, August 10, August 16, and August 17, 1999. The problem occurred during the installation of a software upgrade provided by Lucent technologies for the frame-relay platforms.

A picture of recent intentional cyber intrusions in the United States is provided by the Computer Security Institute's 1999 survey of computer crime and security.²¹ Some 62 percent of the responding private and government organizations experienced unauthorized use of their computer systems during the previous year, with 9 percent being aware of more than 10 incidents. Incidents originated outside for 33 percent and inside for 37 percent of the organizations. Disgruntled employees and independent hackers were most frequently cited as likely sources, although foreign governments too were cited by 17 percent of the respondents. The most frequently reported types of incidents were insider abuse of network access and contamination by viruses. Other incidents included denial of service, system penetration by outsiders, sabotage of data or networks, theft of proprietary information, and fraud. Resulting financial losses to the respondents were estimated to total at least \$124 million, primarily due to theft and fraud. Overall, the survey confirms that vulnerabilities exist and are being exploited frequently.

There are also a number of anecdotes describing deliberate attacks against the computer networks that control critical infrastructure sectors. In 1997, for example, a hacker reportedly shut down a 911 emergency calling system in Florida for an hour, and another hacker disabled vital services to a Federal Aviation Administration (FAA) control tower in Worcester, Massachusetts.²² In another case, a U.S. hacker gained access to the control system for a California dam and reportedly could have released a flood of water, causing considerable loss of life. Fortunately, that was not the hacker's intent. A 1997 DOD military exercise called Eligible Receiver simulated attacks on electric power and telecommunications infrastructure sectors via the Internet.²³ The scripted infrastructure

MCI Worldcom reportedly tried for several days to fix the problem with the network online, but finally was forced to shut down the system and reload an older software version.

21 The Computer Intrusion Squad at the FBI's San Francisco office participated in the survey. The 1999 survey drew 521 responses from a broad spectrum of private and governmental organizations, including 104 from the financial sector. The median organization employed from 1,000 to 5,000 people and had a gross income between \$500 million and \$1 billion per year. The survey results are available at <http://www.gocsi.com>.

22 These examples are recounted in National Research Council, *Trust in Cyberspace*, 18.

23 Eligible Receiver is discussed in President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, 1997, 8. For a skeptical perspective on Eligible Receiver, see George Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology Online*, <http://205.130.85.236/issues/15.1/smith.html>, Fall 1998, 9. Smith notes that the significance of the exercise cannot be determined because the government has not released enough information on its methodology.

attacks, together with hacker attacks on DOD computers, were judged sufficient to disrupt operations at selected military bases and thereby degrade DOD's ability to deploy and sustain military forces.

There is little reliable information on cyber attacks by foreign governments on U.S. infrastructure sectors. While a number of attacks on DOD computers have been reported, these incidents generally have been perpetrated by independent hackers.²⁴ At least initially, the so-called Moonlight Maze episode appeared to be an exception.²⁵ Beginning in March 1999, a number of news publications reported that DOD computers were being probed and information was being stolen by hackers evidently originating in Russia. However, there was no official confirmation that the Russian government was involved and the Pentagon denied that any secrets were compromised.²⁶

The preceding discussion suggests where research and related actions, possibly guided by a new national-level information protection organization, are needed to understand and address the vulnerabilities created by the growing use of networked information systems to manage operations in critical infrastructure sectors. The next chapter explores some vulnerability issues specific to each of several sectors.

²⁴ Several examples are provided in National Research Council, *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, 1999, 18.

²⁵ See, for example, "Networks Attack from Russia?" Reuters, October 6, 1999. Reporting on Moonlight Maze is described and analyzed by the editor of the *Crypt Newsletter* at <http://www.soci.niu.edu/~crypt/other/mmaze.html>. The editor emphasizes that allegations of the involvement of Russian government organizations are attributed to anonymous sources.

²⁶ The Russians nevertheless appear to be engaged in a kind of cyber propaganda war with Chechnya, hacking a Web site that the Chechens use to circumvent Russian censorship of war news. See Paul Goble, "Russia: Analysis from Washington—A Real Battle on the Virtual Front," Radio Free Europe/Radio Liberty (RFE/RL) Newslines, October 11, 1999. Similarly, during the Kosovo conflict, computers at NATO headquarters were spammed by hackers in Serbia in an attempt to disrupt them by overwhelming them with information. There is no confirmation that this unsophisticated attack was sponsored by the Serbian government. See Frank Wolfe, "Pentagon Analyzing Serb Attacks on DOD Web Sites," *Defense Daily*, June 16, 1999.

Chapter 4

VULNERABILITIES IN KEY SECTORS

The critical infrastructure sectors rely on networked information systems that are built in large part of common elements, but specialized, to a considerable extent, to meet the needs of each sector. The research and development necessary to understand and address infrastructure vulnerabilities must, therefore, consider both the general vulnerabilities described in the preceding chapter and the vulnerabilities arising from sector- and even company-specific applications. Thus, as stressed earlier, industry must be closely involved in formulating and executing R&D in this area. This chapter illustrates these points by describing some of the specific issues associated with several important sectors.

We summarize here the findings of recent studies on the Internet, telecommunications, electric power, transportation, and financial services sectors.¹ These studies describe the growing dependence of these sectors on networked information systems and reveal ways that potential vulnerabilities may depend on how systems are used within a sector. How vulnerable these sectors actually are remains uncertain, however, because the published assessments of vulnerabilities typically do not have access to detailed system designs and security methods. As discussed in chapter 3, much more study is needed.

A. INTERNET SERVICE

The Internet is an increasingly important communications mode but is generally viewed as providing inadequate reliability and security.² Moreover, interconnection with

¹ The selection of these sectors for this chapter was based on the availability of suitable published studies.

² See President's National Security Telecommunications Advisory Committee, "Internet Report: An Examination of the NS/EP Implications of Internet Technologies," Network Group, June 1999, 15. (Hereinafter cited as NSTAC-Internet.)

In its study, the PCCIP determined that the public telecommunications network was potentially vulnerable to a major attack:

With network elements increasingly interconnected and reliant on each other, cyber attacks simultaneously targeting multiple network functions would be highly difficult to defend against, particularly if combined with selected physical destruction of key facilities. The possibility that such disruption could cascade across a substantial part of the public telecommunications network cannot be ruled out....No one knows how the network would react under coordinated attack.¹²

The PCCIP noted that more focused attacks, for example on Wall Street or a port of military embarkation, are even more feasible.

1. Existing Vulnerabilities

Telecommunications networks are composed of a number of essential elements:

- Transmission media move signals from point to point. Multiplexing equipment and other automated devices are used to configure and sustain communications paths through these media.
- Switches and routers direct calls and data along the communications paths. They are both software-controlled devices.
- Common channel signaling (CCS) systems are data networks used to set up calls on switched-voice networks, collect billing information, and enable special services.
- Network management systems control, configure, and maintain other network elements. These processes are highly centralized and automated, so that manual network management is now considered to be virtually impossible.¹³

Telecommunications providers have relied heavily on access controls for security. However, anyone who can successfully connect to the advanced operations channels has "virtually unlimited access to everything and everyone connected to them."¹⁴ Potential attackers could affect the operation or configuration of network elements, for example, by altering or blocking network management messages on the CCS system. Attackers could

¹² See President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, 1997, A-7.

¹³ Ibid., A-6.

¹⁴ See Network Reliability and Interoperability Council, *NRIC Network Interoperability: The Key to Competition*, Final Report, July 15, 1997, 110.

disrupt traffic or access, modify, disclose, or destroy information. An attacker could use remote maintenance and test channels to shut down particular pieces of equipment.¹⁵

The risk of attack has increased in recent years because the level of resources needed to mount an attack has fallen. Intruders and their tools have become more sophisticated. Techniques, tutorials, and software-based tools for "script kiddies" are readily available on the World Wide Web. More than a dozen methods of intrusion at the system root level have been identified. Technical descriptions are "generally accurate instructions for exploiting the vulnerabilities of the [public switched network] and network elements, including digital switches."¹⁶

Substantial growth in interconnections among separately owned networks is increasing their vulnerability. The Telecommunications Act of 1996 requires local exchange carriers to grant nondiscriminatory interconnection and unbundled network access to any requesting telecommunications carrier.¹⁷ The intent is to promote competition by enabling new entrants to offer seamless and transparent services across networks. One unintended result, however, is to create an open environment without the requisite security standards and solutions, creating, in turn, "enormous holes in existing security mechanisms and access controls."¹⁸ The number of relatively unknown people and processes with privileged access is increasing. While the public telecommunications network has a history of security exposure, the vulnerability raised by interconnections "over the last decade is without precedent."¹⁹

What is particularly worrisome is that interconnection is unbundled. That is, carriers are granted access to each other's CCS systems and certain management networks. This is much more intimate than simply handing off calls for completion on another network. Other carriers may have access to systems used to operate, administer, maintain, and provision the network. Given the current approach to security, interconnection requires a high degree of trust. If an attacker can penetrate one carrier's

¹⁵ The PCCIP cited a cyber attack on a SONET ring. The attack demonstrated the potential for remote attacks causing widespread outages. See PCCIP, *Critical Foundations*, A-8.

¹⁶ See *NRIC Network Interoperability*, 110.

¹⁷ Actually, the FCC initiated the move to mandatory interconnections in May 1986 when it introduced the Open Network Architecture (ONA). See Karen Olsen and John Tebbutt, "The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security," NIST Special Publication 800-11, August 1995, 2.

¹⁸ See *NRIC Network Interoperability*, 108.

¹⁹ *Ibid.*

communications, collects data, initiates alarms, and transmits application-directed control commands to field equipment. The SCADA host computer may draw information from 30,000 or more data collection points. The EMS also includes an automatic generation control system that manages power generation, for example, originating control signals that instruct generating units to adjust output. The ongoing trend is for utilities to move toward "standard" vendor products using distributed client/server technology but there are also legacy mainframe systems.

2. Control Center Vulnerabilities

The control system is vulnerable to attack through both the control center and the substations. It is also dependent on communications systems that transmit data and control signals.

For a number of reasons, the control center is increasingly interconnected with other networks and outsiders.

- Utilities frequently interconnect their corporate information system with their control centers in order to access control system data. Firewalls or dial-back modems may be used for security.
- There are also operational links among utilities' control centers to implement power sharing agreements, e.g., to balance loads or schedule transmissions. These links have typically been one-way, with proprietary protocols and application-level controls, and have been considered difficult targets. However, a trend toward using standard protocols will enlarge the pool of knowledgeable potential attackers. Links to other utilities are increasing as a result of deregulation, which is placing generation, transmission, and distribution functions in separate companies. These links, too, are driving a movement toward standard, open protocols. Mergers among utilities are also increasing operational links between formerly separate companies.
- Utilities more and more use commercially developed software and outsource its customization and maintenance. As a result, outside manufacturers and integrators are being granted access to control centers through dial-in ports for the purpose of updating software and performing other maintenance.
- Operations and information systems personnel at many utilities can access systems remotely for after-hours troubleshooting, system administration, and maintenance.

The potential harm done by intruders depends importantly on how knowledgeable they are. In general, electronic intruders who gain access to the control center can

potentially crash the EMS. However, most utilities can revert to manual coordination if all control center functions are lost. Intruders who are more knowledgeable may also be able to corrupt billing databases or issue false commands (e.g., open and close relays, shut down lines, and perhaps affect generation). Extremely knowledgeable intruders could manipulate the flow of data to the control center, inducing responses to spurious indications, but very few people have the requisite technical skills and utility-specific knowledge for this.²⁴

3. Other Vulnerabilities

Other vulnerabilities are specific to the substations and field equipment. Many field devices, for example, breakers, switches, and relays, are now remotely programmable. Utility engineers can dial in to the devices and change the settings. An intruder could use this facility either to set a breaker too high and expose protected equipment to physical damage or to set it too low and cause the system to shut down for self-protection. The intruder would have to identify the correct telephone line or port but would not necessarily encounter additional access controls.²⁵ Also, RTUs at the substations often have maintenance ports with dial-up access through which an intruder could issue commands or report spurious data back to the control center.

The communications links underlying the control system are also a source of vulnerability. Perhaps two-thirds of this capacity is typically owned by the utility, mainly microwave and fiber-optic media.²⁶ These lines are not immune to many of the vulnerabilities of public networks. For example, microwave transmissions can easily be jammed using devices described on various Internet Web sites. Further, utilities sometimes sell communications capacity to, and share rights of way with, public networks. When utility control systems do utilize public networks, it is typically for redundancy, for "last mile" connectivity, to access geographically remote regions, or to interconnect with other utilities. In case the communications lines go down, a utility can dispatch operatives with cellular phones or mobile radios to report back information. However, it would be difficult and dangerous to try to restore power in this situation, for example, after an attack on the control system itself.

²⁴ Ibid., 14. Disgruntled employees, current and past, may have the knowledge to cause serious damage.

²⁵ Ibid.

²⁶ Ibid., 15.

In conjunction with deregulation, utilities are now required to post real-time transmission capacity and price information on their open access same-time information system (OASIS) Web site. While utilities typically secure this link between the control system and the Internet, it represents another point of vulnerability to outside access.

D. TRANSPORTATION

The transportation sector is increasingly dependent on networked information systems for both operational and business purposes. Air transport is certainly the most dependent on automated information systems while all modes depend heavily on communications. However, the principal security issues still concern physical threats. Further, the great diversity and redundancy within and among transportation modes limits the potential for nationwide disruption due to natural, accidental, and deliberate incidents. Thus, the NSTAC concluded:

Although a nationwide disruption of the transportation infrastructure is unlikely, even a local or regional disruption could have a significant impact. No single system or critical point of failure is apparent in the transportation infrastructure that could cause disruption on a national scale if destroyed or degraded.²⁷

Passenger transportation, especially by air, has nevertheless proven to be an attractive terrorist target due to the high value placed on human life.

Air traffic control operations clearly depend on networked information systems and communications links with aircraft. This dependence will grow even stronger in the future. The Federal Aviation Administration (FAA), for example, is developing a new nationwide navigation and flight control system, which will be tested as early as next year. This sophisticated system, with air and ground networks linked to on-board computers, will give pilots greater en-route flexibility yet permit closer positioning of aircraft in busy airspace. The system will utilize the Global Positioning Satellite (GPS) system for location information and for an enhanced ground proximity warning system.

²⁷ See President's National Security Telecommunications Advisory Committee, "Transportation Information Infrastructure Risk Assessment Report," June 1999, 58. (Hereinafter cited as NSTAC-Transportation.)

This dependency is a source of concern since questions have been raised about the GPS's susceptibility to jamming, general unreliability, and lack of redundancy.²⁸

Railroads depend on centralized networks for traffic control. SCADAs obtain train location information from sensors on or near tracks and transmit instructions to track-side signaling devices. This has been a largely manual effort, but disruption of SCADAs or control centers could potentially disrupt traffic over wide areas.²⁹ Automation of traffic control has been increasing, with control center computers now controlling track switches and signals for 25 to 30 percent of railroad freight traffic.³⁰ Rail transit systems in major metropolitan areas, e.g., New York City and San Francisco, have similarly been modernizing their traffic control systems.

Information technology is also being focused on improving service for individual shipments. Automated systems are being used to track shipments, sort them at transit points, and improve in-transit routing. Coupled with systems to track trucks, rail cars, and containers, shipment tracking enables more efficient use of resources and better customer service. For example, dispatchers can reroute trucks to optimize shipment pickup and delivery. Disruption of these automated systems could disrupt service at key nodes or lead to lower efficiency and greater congestion.

Transportation companies are increasingly interdependent in providing service for a particular shipment. Inter-modal alliances, for example between trucking and railroad companies, are becoming more important in the effort to provide end-to-end customer service. This requires more companies to exchange information on passengers, cargo, and operations. Some companies, such as Federal Express and United Parcel Service, provide end-to-end service using their own inter-modal facilities and dedicated high-speed data networks.

Transportation companies in all modes are moving from closed proprietary networks to open, interconnected networks to provide value-added information for their customers and suppliers. Increasingly, customers can make reservations or track shipments electronically, often via the Internet. This information, together with quick,

²⁸ Evidently, the threat that hackers could alter the trajectory of the satellites has proven exaggerated. See NSTAC-Transportation, 54.

²⁹ Incompatible computer systems were blamed for months of severe congestion when Union Pacific and Southern Pacific Railroads merged. See John Dodge, "Can IT sink a merger? We're bound to find out," *PC Week*, June 22, 1998.

³⁰ See NSTAC-Transportation, 21.

reliable, and agile service, is essential for businesses that rely on just-in-time inventories and advanced supply chain management methods.

Automated systems are also being used to facilitate compliance with regulatory requirements. For example truckers can be monitored for compliance with highway safety procedures. Automated systems are in place for clearing customs and satisfying roadside weigh station requirements. Disruption of these systems could lead to local congestion.

Aircraft and a substantial portion of rail freight operations depend on automated traffic control systems. The efficiency and quality of service for all modes depends on automated systems that track shipments and equipment. At the same time, competitive pressures and new business practices are leading to more networked interconnections between transportation companies and their customers, suppliers, and peers. Operations and efficiency are thus vulnerable to attacks on automated information systems. Future trends promise more dependence on information technology and, perhaps, greater physical concentration of transportation resources at key inter-modal transit points.

E. FINANCIAL SERVICES

The financial services sector is almost completely dependent on networked information systems to process a huge volume of transactions and keep track of the assets of millions of customers.³¹ At the same time, the sector is exceptionally focused on managing its security risks. This emphasis stems from the need to maintain customer trust, the potential for business losses due to disruptions, and the concerns of financial regulators. In studying the sector, the NSTAC determined that financial institutions have implemented "extensive layers of technical and procedural controls that put significant cyber attacks outside the scope of all but a long-term concerted nation-state effort."³²

Many of the institutions interviewed for the NSTAC study "voiced the concern that they could not manage against cyber threats on the scale of an 'electronic Pearl Harbor'

³¹ The financial services example is based heavily on President's National Security Telecommunications Advisory Committee, "Financial Services Risk Assessment Report," Infrastructure Assurance Task Force, December 1997. (Hereinafter cited as NSTAC-Finance.) That report defines the sector to include banks and other depository institutions, investment-related companies, industry utilities, third-party processors, and other services. It does not consider insurance, consumer finance, or mortgage companies since disruption of their networks would not have an immediate national impact.

³² The NSTAC study notes that misleading media reports have generated a false popular impression of vulnerability to cyber attack. The sector's penchant for withholding detailed information has contributed to this view. See NSTAC-Finance, 52, 58.

because they had no credible evidence that these threats existed."³³ Further, they viewed the greatest threat to financial infrastructures to be physical destruction, not cyber attack.

The dependence of financial services on networked information systems is nevertheless breathtaking. In the last decade or so, automation of payment and market systems has enabled an enormous increase in the volume and the velocity of financial transactions. Electronic services now include direct deposits of salaries and other payments, automated teller machines, verification of debit and credit cards, electronic funds transfer, and online securities transactions. Competition in the sector is intense, driving the introduction of new services and challenging security capabilities.

1. Core Payments Infrastructure

The electronic payments, clearing, and settlement institutions are among the most critical segments of the financial infrastructure.³⁴ While cash and checks still dominate transactions volume, virtually all large-value payments and exchanges are made electronically. Interbank payments depend on the Fednet, a data network that interconnects the Federal Reserve Banks. Some 11,000 institutions are connected to the Fednet by dedicated or dial-up lines. The Fednet enables the Fedwire service for real-time funds transfers among banks and other depository institutions. Fednet is also used for electronic "book-entry" transfers of government securities and has largely enabled the Federal Reserve to eliminate paper government securities. Wire transfers are often considered to be vulnerable since they are interactive and involve large sums of money. However, protective measures include the use of highly structured transfer messages, strong encryption, authentication, and secure customer connections. Further, the financial institutions that originate wire transfers have stringent internal procedures to control them, for example, requiring multiple confirmations. The backbone network itself is robust, including online backup centers that can recover functions within minutes of a failure of a primary site.

The Federal Reserve provides most automated clearing house services. Financial institutions forward batches of transactions via Fednet to processing centers for clearing and settlement against other institutions. Transactions include, for example, direct billing payments and direct deposits of payrolls, dividends, pensions, and benefits.

³³ NSTAC-Finance, 27.

³⁴ Ibid., 16.

Other core payments systems include the Clearing House Interbank Payments System (CHIPS), which is the primary processor for international dollar payments and the major clearing system for foreign exchange transactions. Some 104 participants are linked to the CHIPS data center by dedicated data lines. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) provides a secure international payment message system that carries, for example, instruction messages for payments made via CHIPS.

The bank credit card systems, Visa and MasterCard, oversee complex networks to authorize and process transactions. Countless point-of-sale terminals are linked by dedicated or dial-up lines to a network of third-party processors, card associations, and banks.

2. Banking Systems

Banks have taken a conservative approach to adopting new technologies. While competition and new opportunities have driven them to provide many new cyber services, they have implemented these services with a careful eye on their security implications.

Mission-critical banking applications still rely overwhelmingly on legacy mainframe computers and related protocols. The NSTAC study found little indication that this would soon change.³⁵ For a number of reasons, the mainframe systems are considered more secure, reliable, and manageable than new client/server technologies being adopted for other functions. Most importantly, mainframe technology is mature and its vulnerabilities are understood. Further, because legacy software systems tend to be proprietary or customized with little or no online documentation, planning an attack would require much time and effort. The procedures, protocols, and applications would be very difficult for an untrained person to understand or execute. The mainframe systems are also considered easier to control and easier to recover at backup sites in the event of a primary site failure. Computer viruses too are less of a threat. Cost and performance advantages nevertheless are leading banks to implement TCP/IP client/server networks for many non-core applications.

Banks have exposure to outsiders through both remote access and outsourcing. Remote access to at least some of a bank's systems is used for telecommuting, customer services, and administration and maintenance by staff or vendors. Banks increasingly outsource such functions as software development, network management, and transaction

³⁵ Ibid., 50.

processing. Further, banks are not always successful at extending their security policies to their vendors. For example, consultants and contractors who work alongside bank employees may not have been screened as thoroughly.

Online banking is growing rapidly, forcing banks to confront the security implications of using the Internet. Already, 39 of the largest 100 banks are offering at least the minimal banking functions of online bill payment, account status, and account transfer.³⁶ While early schemes utilized direct dial-up lines, access via the Internet is increasingly common. In either case, bankers are wary and limit their risk by screening transactions, limiting transaction values, and using encryption for authentication and privacy. Most importantly, bankers are isolating their customer interfaces and Web sites from their sensitive internal systems. Sites providing account information and financial transactions are not directly linked to a bank's actual cash management systems. For example, data may be exchanged only once or twice per day, typically by manual batch file transfers.

Most major institutions have backup data centers they can switch to in the event of a primary center outage. Data centers may also have uninterruptible power sources, generators, and on-site fuel storage. Data files may be copied and stored off-site. Because of their great dependence on communications, banks typically seek diversity of carriers and routes for both local and long-distance links.

3. Securities Market Systems

Stock markets and commodity exchanges too are heavily dependent on networked information systems and have a high concern for security. Huge volumes of transactions must be processed and trusted ownership records must be kept. Explosive transactions growth has been enabled by the adoption of new technologies.

The securities infrastructure includes core centers for clearing and settling trades, for example, the National Securities Clearing Corporation (NSCC) and the Government Securities Clearing Corporation (GSCC).³⁷ As a procedural control, trades are executed only after confirmation from both buyer and seller. Functional disruption of a settlement

³⁶ See "Is Online Banking Ready for Your Money?" *NetGuide*, <http://www.netguide.com/Snapshot/Archive?guide=money&id=164>, October 31, 1999.

³⁷ Clearing confirms the key information for a trade, i.e., the identity and quantity of the item traded, the price and date of the trade, and the identity of the buyer and seller. Settlement is the exchange of payment for the item traded. See NSTAC-Finance, 18.

organization would probably force a halt to trading on the exchange being supported. The Depository Trust Company (DTC) acts as the securities custodian, using an electronic book-entry system to record ownership. Most securities now are exchanged as book entries rather than paper certificates.

Traditional stock markets conduct trading on the exchange floor. The NASDAQ, however, is an electronic communications network that consolidates dealer quotations and enables electronic trading. NASDAQ order entry and execution has nevertheless typically been done by telephone. Increasingly, brokers are offering online services for taking orders for the major exchanges.

F. VULNERABILITIES AND THE RESEARCH AGENDA

The PCAST proposed the LNIIP as a focal point for identifying and addressing infrastructure vulnerabilities. The required research must examine the general issues associated with networked information systems as well as the specific challenges posed by the application of these systems within each infrastructure sector and between critical infrastructure sectors.

This research requires access to information held by both the government and the private sector.³⁸ The government has responsibilities for identifying threats as well as valuable experience in protecting its most sensitive networked information systems. However, as the PCCIP notes, only the owners and operators of the critical infrastructures have the knowledge, access, and technology needed to defend their systems.³⁹ There is a need to understand the vulnerabilities in U.S. infrastructure sectors, and to do this, a way must be found for the government and private sector to work collaboratively.

³⁸ Some observe that much of the information needed does not exist, while that which does exist is often not shared because it is classified or proprietary. See Stephen J. Lukasik, "Protecting Information-Dependent Infrastructures," *Information Impacts Magazine*, <http://www.cisp.org/imp/>, September 1999, 4.

³⁹ See PCCIP, *Critical Foundations*, 24.

Part III

Functions Needed for Infrastructure Protection

Chapter 5

FUNCTIONAL ASSESSMENT: OVERVIEW

This chapter focuses on each of the functional areas that have been identified for strengthening infrastructure protection. In each functional area, we draw on the results of our interviews and workshops to describe the nature of the functions that need to be performed in greater depth. We then consider the degree to which existing organizations are performing some or all of these functions, or are engaged in closely related activities. The purpose is to better delineate the needed functions, and then to determine whether it makes the most sense to assign a function to an existing organization or to place it in a new organization.

This chapter introduces our approach. It describes the functional areas reviewed and identifies the organizations that are assessed in this section.

A. THE FUNCTIONAL AREAS

The functional assessment focuses on one overarching management function and four programmatic functional areas. The programmatic functions include research and development, information sharing, product evaluation, and educational initiatives. (See figure 5-1.) The successful performance of these functions is necessary to meet the R&D-related goals set forth in Presidential Decision Directive 63, and elaborated upon by the PCAST proposal.

Our interviews and workshops revealed general support for this taxonomy of functions, and broad agreement that more can and should be done in each area.

The Study Team reviewed available documentation to determine each organization's mission and functions and assessed the degree to which the organization is now performing one or more of the functions identified in table 5-1. We addressed the following general questions:

1. Who's doing these functions now? How well? (Specific organizations/activities).
2. What elements are not being performed? Are there known shortfalls or gaps?
3. What changes to current organizations would yield the desired results? Are they feasible?
4. Do we need a new entity to perform functions not being addressed or being done poorly? What are the arguments in favor of and against formation of a new entity?
5. Do we need to provide an integrated national central focus for the function, and if so, how?

Table 5-3 identifies the current activities that we reviewed within each of the functional areas. This table includes the largest and most significant organizations performing functions in this area, but it is not exhaustive. Hundreds of related programs and activities are under way across these organizations, and one must examine individual units to understand the full range and applicability of ongoing activities.

Table 5-3. Organizations Reviewed in Each Functional Area

<u>Research and Development</u> Private Sector (EPRI, Telcordia) Universities (Purdue, INFOSEC centers of excellence.) Government (NSA, DARPA, NIST, NSF, DOD Laboratories, National Laboratories)	<u>Information Sharing</u> Private Sector (FS-ISAC) Universities Government (CERTs, NIPC, NSTAC-NSIE)
<u>Product and Service Evaluation</u> Private Sector (BITS laboratory, ICSA) Universities Government (NSA, NIST, NIAP) Accreditation ((ISC) ² , ISACA) Standards (ANSI, IETF)	<u>Education and Training</u> Private Sector (AFCEA, CISCO, etc.) Universities (INFOSEC Centers of Excellence, Naval Postgraduate School) Government (NSTISSC, NSF)

The baseline review gave us an appreciation for the broad scope of ongoing activity in the public, private, and academic sectors on cyber infrastructure protection issues, and initiatives. With this perspective, we summarize our analysis in the following chapters.

Chapter 6

RESEARCH AND DEVELOPMENT

R&D will be the principal function of the proposed I3P. The view that the nation's R&D efforts need substantial strengthening is, of course, the central motivation for the PCAST's proposal to create a new R&D organization. The public and private sectors are funding a great deal of information assurance research, and their investments in this area have grown significantly in recent years. These efforts nevertheless still fall short of what is required, and some experts believe that the Nation's vulnerabilities to cyber attacks are growing faster than ever before. There is a widespread view that funding is inadequate now for R&D focused on understanding and addressing the vulnerabilities in the Nation's critical infrastructure sectors. More research is needed to identify and address such vulnerabilities, especially those that expose infrastructures to large-scale, coordinated attacks that could have catastrophic consequences. A national focal point is required both to coordinate the research that is being done and to ensure that priority requirements are met. This chapter reviews current activities and identifies the roles that the I3P should perform.

A. R&D REQUIREMENTS

Several systematic reviews have identified the kinds of R&D that are needed, and have outlined these requirements in formal R&D roadmaps. This section summarizes the current understanding of R&D requirements. This starting point was then used to determine the extent to which current activities are meeting R&D needs, and to determine which tasks ought to be assigned to a new organization.

1. PCAST Proposal

The PCAST saw a need for a dedicated, well-staffed national laboratory focused on assuring the long-term cyber security of the nation's critical information infrastructure.

Accordingly, it proposed the establishment of a new not-for-profit organization, in the private sector, to conduct research and develop technology to—

- Protect against penetration and damage, natural instabilities, internal design weaknesses, and human failings
- Gain a systematic understanding of vulnerabilities
- Develop a broad understanding of the robustness and resiliency of complex systems
- Create the means to assure graceful degradation under stress

2. IDA Interviews and Workshops

The IDA interviews and workshops indicated that much of the commercial research and development in the information assurance field is driven by near-term market opportunities. Within the government, most R&D is funded by the Department of Defense, and the focus is generally on the government's infrastructures.

While the appropriate nature of the research agenda (i.e., basic science, large-scale systems architectures, or product engineering) remains to be determined, there is general agreement on the need to fund long-term basic research, especially to identify and address the vulnerabilities associated with complex interrelated systems. University experts particularly focus on the need to establish a "science of information security" that could develop a deeper understanding of how information networks operate and where their important vulnerabilities lie. In addition, industry and university representatives frequently expressed the concern that much more systematic thought needs to be given to the forensic, legal, and judicial implications of the information age.

Apart from concerns with the gaps in current R&D activities, there is a general concern over the lack of effective mechanisms for disseminating and making new research results widely available. This has prevented effective exploitation of the research currently being done. Such communications gaps also inhibit the establishment of a coherent research agenda that effectively identifies and prioritizes gaps and limitations in the current state of knowledge. Nevertheless, industry seems willing to cooperate with government to develop and coordinate research roadmaps and agendas, a task that industry, government, and academic experts agree the government is best positioned to sponsor.

In addition, most of those interviewed agree that government should take the lead in raising awareness of the risks associated with infrastructure vulnerabilities. Executives interviewed for this study indicate that their companies are increasingly aware of the risks

associated with day-to-day hacking and criminal attacks, but they generally do not consider the risks associated with larger, orchestrated attacks such as might result from cyber terrorism or cyber attacks mounted by a nation state.

3. R&D Roadmaps

The R&D needs identified by the PCAST proposal and reinforced by the IDA review are consistent with several detailed reviews and roadmapping activities performed in recent years. These activities are highlighted here to provide context for our study, as well as to suggest the logical starting point for subsequent efforts to develop a detailed assessment of the unmet R&D needs in this area. The required R&D areas identified in each review are summarized here and arrayed in Table 6-1.

- *Critical Infrastructure Protection R&D Interagency Working Group* (CIP R&D IWG) capitalized on the "Preliminary R&D Roadmap for Protecting and Assuring Critical National Infrastructures" prepared for the Transition Office of the PCCIP. This effort identified and examined some 71 R&D programs in six broad infrastructure categories across all the sectors.
- *Argonne National Laboratory* coordinated preparation of a report for the PCCIP, "Technology R&D Roadmap for Protecting the Information and Communication Infrastructure." This study identified four major research thrust areas and 13 prioritized R&D needs.
- *Sandia National Laboratories*, aided by industry experts prepared "U.S. Infrastructure Assurance Strategic Roadmaps" for the Transition Office of the PCCIP. This sector-by-sector review assessed the vulnerabilities of the critical infrastructures and recommended protection strategies. It sets forth six roadmaps designed to guide the improvement of infrastructure surety and serve as strategic plans for the development and introduction of technologies and policies into each of the critical sectors. A key priority is to research, develop, and deploy advanced communications and information technologies and systems to address vulnerabilities.
- *Trust in Cyber Space* documents a review of R&D needs performed by the *National Academy of Sciences/National Research*. This is an extensive examination of networked information systems, their vulnerabilities, and alternative solutions. The book provides a detailed agenda for the conduct of research to address the trustworthiness of networked systems.
- *Software Engineering Institute (SEI) at Carnegie Mellon University* proposed an Information Assurance Research Institute (IARI) that would follow a careful, systematic approach in developing technologies needed for cyber protection of the national information infrastructure across all the connected

sectors. The scientific element of the program would produce validated theories and hypotheses as a basis for development of an engineering discipline of practices, methods and tools. An engineering segment would provide feedback to the science research on the implications and applicability of research results. The evolving science foundation and engineering discipline would form a body of knowledge to drive education and technology transfer programs in a laboratory environment.

Table 6-1. Roadmaps for Information Assurance R&D

CIP R&D IWG 1988 R&D Options	Argonne/PCCIP Thrust Areas	Sandia/PCCIP Sector Roadmaps	Trust in Cyberspace	SEI IARI Proposal
Vulnerability Detection and Analysis Intrusion Detection and Warning Authentication Technologies Artificial Intelligence Simulation Tools and Models Interdependency Analyses Trend Analyses Response and Recovery Technologies Test Facilities	Risks, Threats and Vulnerabilities Intruder Incident Detection, Response and Recovery Building High Confidence Infrastructures Modeling and Simulation	Communications and Information Electric Power Oil and Gas Banking and Finance Transportation Emergency Services	Software Design and Planning System Integration and Assurance Access Control Identification and Authentication Systems Cryptography and Public-Key- Infrastructures Network Access Control Operating system Security Types of Firewalls	Create and validate a science of Information Assurance Develop a science- based engineering discipline Conduct policy development, technology transfer and education to improve the state of the art and practice of Information Assurance

While the first three studies derived their recommendations by examining the needs of particular infrastructure sectors, the R&D topics in Table 6-1 are largely generic. That is, they address R&D activities that are applicable across all infrastructure sectors, rather than focusing on the specific needs of individual sectors.¹ One issue that will have to be addressed in defining R&D needs is to determine the appropriate balance between

¹ To gain a sense of how needs differ among the sectors, it is instructive to sample some FY 2001 R&D options compiled by the CIP R&D IWG:

- Banking and finance (physical protection technologies, metrics for the banking and finance infrastructure)
- Information and communications (radio spectrum infrastructure vulnerability, enhanced JAVA security)
- Energy (energy system complexity analysis, metrics for the energy infrastructure)
- Transportation (controller-pilot data link communications security, intermodal cargo security)
- Vital human services (risk assessment of water supply system, systems analysis of public health emergency response systems)

to be addressed in defining R&D needs is to determine the appropriate balance between R&D that focuses on problems that cut across all sectors, and problems that are unique to individual sectors.

4. Needed R&D Functional Tasks

Our review finds broad agreement on the kinds of R&D that are needed to identify and address infrastructure vulnerabilities. The main elements of an overall national program are discussed below.

First, the breadth of proposed research topics ranges from building a scientific foundation to creating many kinds of here-and-now technologies. This range is illustrated in Table 6-2, which presents a research framework developed for an earlier IDA study.² In this framework, fundamental research is needed to build a scientific foundation to support system-level engineering, which is necessary to integrate individual components into secure systems and networks. As discussed below, existing research tends to focus on component development, particularly in the private sector. The need for system-level engineering may be even more urgent, but it is a very difficult area that lacks a scientific foundation. For the critical infrastructure sectors, any requirements for sector-specific research are most likely to fall under the headings of system engineering and component development.

Table 6-2. Framework for Information Assurance Research

Basic Research in IA Fundamentals	System-level Security Engineering	Individual Component Development
Protection Concepts & Principles	System Architecture	Security Management
System Complexity Issues	Heterogeneous Component Integration	Intrusion Detection
Vulnerability Analysis	Secure Interoperability and Evolvability	Identification and Authentication
Trust Concepts	Applied Engineering Research	Smart Cards
	System Assurance	Networking
	Standards	Applications
		Secure Operating Systems
		Applied Cryptography
		Hardware-based Security

² See William T. Mayfield et al., *Commercial Perspectives on Information Assurance Research*, IDA Paper P-3359, October 1997, 24.

The breadth of needed research raises questions about priorities and, in particular, about what research will best support protection of the cyber systems of the critical infrastructure sectors against large-scale attacks with catastrophic national consequences. Moreover, it suggests a need for ongoing mechanisms to set priorities and to ensure that the national R&D agenda is suitable. Another important point is that R&D requirements are sometimes specific to an infrastructure sector, sometimes the same for multiple sectors, and sometimes involve interdependencies among sectors. The research agenda must address issues within individual sectors, but it must also reflect a broader perspective that integrates across sectors and considers the cascading effects of attacks. In sum, there is a need for a national-level R&D agenda with a strategic focus.

The national research program must be grounded in an understanding of the information infrastructures of the critical infrastructure sectors. In particular, they should be studied and characterized as interdependent national information infrastructures, as a system of systems. This perspective is essential for gaining a strategic understanding of high-level threats, vulnerabilities and protection needs.

Further, to support the formulation of a national research agenda for protecting the cyber systems of the critical sectors, ongoing research should be monitored in both the public and private sectors. Tracking research plans is necessary in order to identify serious gaps and shortfalls. Tracking research progress is important for spotting technical opportunities.

The following section reviews ongoing R&D activities, and attempts to determine which aspects of this overall National program are being addressed today. As we shall see, some important R&D areas are not being adequately addressed today. There is a need to fund research in new or unconventional areas (e.g., basic science, information assurance principles, standards, and tools) that are currently unlikely to find support through existing R&D mechanisms.

B. EXISTING R&D ACTIVITIES

As noted earlier, R&D expenditures are growing in both the private and public sectors. The magnitude of private sector R&D is not known with any degree of precision. In a 1997 survey, Mayfield et al. estimated the information assurance R&D expenditures

of 12 major IT corporations to be in the range of \$200 to \$500 million.³ This is an incomplete estimate, and given the rapid growth of sales in this area, R&D spending can be expected to have increased in these firms since 1997. The R&D being performed by industry is focused predominately on the development of next-generation product releases, and therefore has been very near-term in perspective. Executives interviewed for this study indicated that the fast pace of the competitive marketplace simply did not allow them to focus beyond near-term market requirements.

The kinds of products being developed by industry include firewalls, intrusion detection devices, networking components, smart-card technology, cryptography applications, and other security management tools.

At the federal level, the budget request for R&D to support critical infrastructure protection amounts to almost \$500 million. The major government R&D programs are described below.

1. Government Infrastructure Protection R&D Activities

Table 6-3 shows that most of this federal funding is provided through DOD programs

**Table 6-3. FY2000 Government Agency Budget Requests
for Critical Infrastructure Protection R&D**

Agency	Funding (\$M)
Defense	352.0
Transportation	57.0
Energy	36.4
National Science Foundation	18.4
Commerce	11.4
Interior	4.0
Justice	3.4
National Aeronautics and Space Administration	2.6
Total	485.2

³ William T. Mayfield, Ron S. Ross, Stephen R. Welke, and Bill Brykczynski, *Commercial Perspectives on Information Assurance Research*, Institute for Defense Analyses, IDA Paper P-3359, October 1997. These estimates are based on industry reports that they were devoting about 1% to 3% of their total R&D on information assurance issues.

a. Critical Infrastructure Protection R&D Interagency Working Group (CIP R&D IWG)

At the national level, the Office of Science and Technology Policy (OSTP) is responsible for coordinating R&D agendas and programs across the government. In the infrastructure protection area, OSTP does this through a working group under the National Science and Technology Council (NSTC). This working group is the CIP R&D IWG. It is responsible to both the National Security Council (NSC) and the NSTC. (See Figure 6-1.)

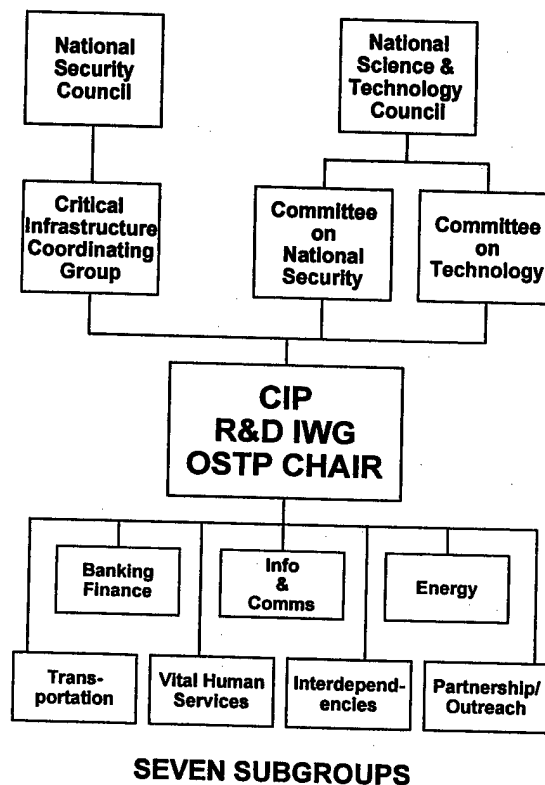


Figure 6-1. Critical Infrastructure Protection R&D Interagency Working Group

The CIP R&D IWG is charged with:

- Monitoring and coordinating ongoing and planned government R&D
- Fostering conditions for developing a close R&D partnership with the private sector, academia and international groups
- Facilitating transfer of technology from government agencies to the private sector

The CIP R&D IWG is examining R&D options across several infrastructure sectors (i.e., Banking and Finance, Information and Communications, Energy, Transportation, and Vital Human Services), identifying high priority cross-cutting common needs, and sponsoring R&D workshops.

Two other offices also play a role in coordinating federal R&D in this area. The first is the National Coordinating Office for Computing, Information, and Communications R&D (NCO/CIC). It works to develop and implement government-wide R&D agendas in designated program areas. Examples include the High-Confidence Systems (HCS) working group, and the Large-Scale Networking (LSN) working group. Although information assurance is not an NCO program area, many of the same officials are involved in both the NCO and the CIP-IWG, and many of the program issues are closely related. A second office that assists in coordinating R&D is the Critical Infrastructure Assurance Office. The CIAO provides support to the National Coordinator for Critical Infrastructure Protection and Counterterrorism.

b. Department of Defense (DoD) Activities

Table 6-3 indicates that most of the government's R&D funding is provided by the Department of Defense. The Defense Advanced Research Program Agency (DARPA), NSA, and the Military Departments are the principal sources of funding. Recently the DoD established the Defense-Wide Information Assurance Program (DIAP) to coordinate activities across the Department. These DoD activities are reviewed here.

Defense-Wide Information Assurance Program (DIAP)

The DoD Chief Information Officer (CIO) has department responsibility for information assurance and uses the DIAP as the mechanism to carryout that role. With respect to research and technology, the DIAP provides for R&D of information assurance technologies consistent with current and anticipated mission needs. The intent is to leverage research throughout DoD, the government, the private sector, and academia.

Defense Advanced Research Projects Agency (DARPA)

DARPA is a DoD agency charged with the mission of maintaining U.S. technological superiority across a broad range of R&D fields. Its Information Technology Office (ITO) and Information Systems Office (ISO) are pursuing initiatives related to detecting cyber attacks against networks, countering the attacks, and repairing the damage. The chief mechanism used by DARPA is to fund a broad swath of external

research projects through a series of Broad Area Announcements (BAAs), which are calls for proposals from industry. Currently, BAAs have been released for several hundred million dollars in information technology and information assurance study areas.

DARPA programs address both component technology and network-level information assurance. In recent years, for example, DARPA has managed component technology programs for:

- Intrusion detection and response, including developing algorithms, protocols, and software
- Boundary controls, including domain and type enforcement firewalls and alertable firewalls
- Authentication methods, including wireless identification systems, certificate authority workstations, and the security services desk concept
- Dynamic virtual private networking
- Wrappers, to enable the secure use of legacy operating systems

A major new program will address information assurance and survivability at the network level, aimed particularly at providing security and survivability for DOD's next generation information infrastructure. Among other things, this effort will develop:

- Network security architectures, integrating component technologies
- Information assurance science and engineering tools, developing an underlying science that permits a formal understanding of information assurance problems, enabling the creating of metrics, methods, and tools to support both the design and assessment of information systems
- Intrusion tolerant systems, including architectures and techniques to enable the fielding of systems that respond to intrusions with actions that ensure continued correct and timely user services even in the face of an attack
- Cyber command and control techniques, including a strategic cyber decision support system to help commanders thwart information warfare campaigns while maintaining operational functions
- Autonomic information assurance, including a distributed operational systems control framework to detect and tactically respond to defined classes of attacks autonomously

DARPA's programs are executed through private contractors, universities, and national laboratories. The work is designed to support the protection of DOD's information systems and is specialized to some degree for military situations and

particular types of systems. In many cases, however, the results may also prove useful for the protection of civilian infrastructures and generic information systems.

c. National Security Agency (NSA)

This DoD agency's primary mission is to provide signals intelligence and communications security activities for the government, including DoD information systems security and operations and security training. The NSA's Information Systems Security Organization (ISSO) has the responsibility for information security matters and uses its National Computer Security Center to assist in security research efforts. A broad INFOSEC technology program is underway to achieve five basic objectives:

- Anticipate emerging information technologies and design programs and architectures for the development of security solutions
- Build a broad INFOSEC knowledge base through advanced research in information processing, communications and security technologies
- Develop, test, and demonstrate new approaches to information security
- Coordinate national INFOSEC R&D activities
- Preserve cryptographic preeminence

Specific research topics are detailed in NSA's Information System Security Research Program Plan, which describes work in 41 separate technical areas directly related to cyber protection of infrastructure resources. Examples include:

- Network Boundary Identification
- Security Implications of Physical Layer Changes
- Biometrics
- Trusted Operating System Prototype
- Damage Taxonomy
- Detection Taxonomy
- Recovery Taxonomy
- Public Key Cryptography
- Quantum Cryptography
- High Speed Security
- Formal Methods
- Anti-tamper Techniques
- Risk Management Tools

Supporting NSA activities include:

- *Advanced Research and Development Activity (ARDA)*. It was established to independently formulate strategic goals and guidance for a strategic plan for advanced R&D in information technology. ARDA is pursuing research to develop algorithms, techniques and enabling core technologies in nine separate information technology thrust areas.
- *INFOSEC Research Council (IRC)*. Sponsored by NSA, other participants are DARPA, NIST, DOE, NSF, and the Military Services. The IRC objective is to share the details of information security and information assurance R&D programs across government, universities, and contractors, focusing on R&D topics.
- *Information Operations Technology Center (IOTC)*. This NSA based center is focused on developing tools and techniques needed to conduct information warfare. It was established in March 1997 by the SECDEF and DCI to respond to the need for a single center to integrate diverse service and intelligence community offensive information operations technology efforts, and to establish and maintain a national repository of these techniques.

d. Military Departments

The Military Services fund a range of information assurance R&D activities in their laboratories. The Naval Research Lab, Air Force Rome Labs, and the Army Research Labs are examining basic and applied research efforts on a variety of topics directly related to information and infrastructure protection goals. They participate in DoD fora and interagency efforts to exchange and coordinate ideas and best practices.

2. Department of Energy

The Department of Energy funds R&D on infrastructure protection at the National Laboratories. In addition, the laboratories' development of advanced computing and networking to support the Stockpile Stewardship Program has necessitated developing information assurance technologies and methods. The National Laboratories therefore represent a major source of technical expertise in this area.

Sandia operates DOE systems engineering laboratories whose primary mission is guaranteeing the surety of the nuclear weapons stockpile. Additionally it has the mission to improve the surety of the nation's energy infrastructure. Sandia used its

multidisciplinary technical capabilities to assist the President's Commission on Critical Infrastructure Protection (PCCIP) in areas such as:

- Coordinating infrastructure assurance strategic R&D roadmaps with the private sector.
- Modeling interdependencies of the critical infrastructure to identify system interactions and predict responses to disruptions.
- Examining information assurance technologies for key management systems, cryptography, authentication, high surety hardware/software, monitoring, and detection systems.
- Conducting vulnerability assessments and systems analysis to identify critical nodes and networks.
- Conducting research at Argonne National Laboratories to address basic science (including computer science), scientific facilities, energy resources, and environmental management. Argonne took the lead for coordination of the PCCIP report on an "R&D Roadmap for Protecting the Information and Communications Infrastructure in the U.S."

Lawrence Livermore and Los Alamos National Labs each have extensive information assurance programs developed to protect highly sensitive data and computer codes used in nuclear weapon design.

3. Department of Commerce

The Department of Commerce (DOC) has a multifaceted role with respect to national information infrastructure protection:

- Establishing partnerships with the private sector to develop and advance dialogues and activities to improve infrastructure security.
- Operating the National Institute of Standards and Technology (NIST) designed to meet the cyber security testing requirements of Information Technology users and producers, public and private.
- Providing the resources for the operation of the Critical Infrastructure Assurance Office (CIAO), which is charged with integrating private sector plans into a national infrastructure assurance plan and coordinating analyses of critical infrastructures.

Each of these endeavors is being pursued vigorously. The DOC has reached organizational agreements with several Private Sector Coordinators [e.g., Telecommunications Industry Association (TIA), Information Technology Association of

America (ITAA), United States Telephone Association (USTA)]. Recently DOC has also created an industry-government alliance called the "Partnership for Critical Infrastructure Security" which includes more than 80 leading companies and industry associations (e.g., Microsoft, AT&T, Cisco Systems, Citigroup, Consolidated Edison).

NIST operates an Information Technology Laboratory (ITL) which concentrates on developing tests and test methods for information technologies to provide impartial means of measuring to assist developers and users in product evaluation based on objective criteria. The ITL assists the National Information Assurance Partnership (NIAP), a NIST collaboration with the National Security Agency to meet the security testing requirements of both the public and private sectors. The NIAP develops tools, test methods, and tests for specification-based information technology security products. They serve as the nation's center of expertise and resources for the security testing community.

As noted earlier, the CIAO provides support to the National Coordinator for Critical Infrastructure Protection and Counterterrorism in the National Security Council staff structure. Its chief activities include the drafting of a National Plan for Infrastructure Protection, promotion of private sector led information sharing and public-private partnership arrangements. The National Plan reportedly covers the following 10 principal areas of interest:

- Identify and address vulnerabilities
- Detect and respond to attacks
- Create/maintain/coordinate law enforcement capabilities
- Share information on warnings and attack with private sector
- Create capabilities for response, reconstitution, and recovery
- Promote research and development
- Promote training and education
- Conduct Outreach Programs to educate private sector
- Ensure industry's privacy in information sharing program
- Review aggregate budgets and potential organization for national IA.

4. National Science Foundation

The National Science Foundation (NSF) is an independent agency of the U.S. government with the mission of promoting science to advance national health, prosperity, welfare, and defense. The focus of interest for national information infrastructure protection is its Directorate for Computer and Information Science and Engineering (CISE). The NSF has recently awarded some 50 grants related to information technology (IT) in topic areas such as the following:

- A project to increase competition in naming internet domains
- High data rate wireless internet connections
- IT research in a competitive world
- Development of an undergraduate major in IT

The NSF essentially administers grants, contracts and R&D programs to foster the interchange of scientific information, methods, technologies and research. Its Director is appointed by the President and it reports to the National Science Board comprised of 24 members. The NSF fulfills its mission by also performing the following activities:

- Award fellowships to perform research in selected areas
- Foster development and use of computers and other scientific methods and technologies, primarily for research and education in the sciences
- Evaluate status and needs of the various sciences and engineering and correlate research and educational programs with other Federal and non-Federal programs
- Maintain register of scientific and technical personnel. Provide a clearinghouse for collection, interpretation, and analysis of data on scientific and technical resources and provide information for policy formulation by other Federal agencies
- Determine amount of Federal money received by universities, et al, for scientific and engineering research, including basic and applied
- Initiate and support specific scientific and engineering activities relating to international cooperation, national security, and the effects of science and technology on society
- Initiate and support scientific and engineering research, including applied research, at academic and other nonprofit institutions

- Recommend and encourage the pursuit of national policies for the promotion of basic research and education in the sciences and engineering; strengthen research and education
- Support activities designed to increase the participation of women and minorities and others under-represented in science and technology

5. Other Organizations

A number of other government organizations are also involved in efforts to improve the security of their infrastructure resources and, as noted earlier in Table 6-2, have submitted budget requests for Critical Infrastructure Protection R&D funding.

The Department of Transportation (DOT) consists of eleven individual operating administrations including the Federal Aviation Administration, the Federal Highway Administration, the Federal Railroad Administration, Maritime Administration, and the Research and Special Programs Administration, which operates the Volpe National Transportation Systems Center in Cambridge, Massachusetts. The Volpe Center is dedicated to enhancing the effectiveness, efficiency and responsiveness of other Federal organizations with critical transportation-related functions. DOT's Information Technology Security Service Bureau is responsible for providing services to protect automated information and IT assets from threats and vulnerabilities. They offer a range of security services to include risk analyses, security plan development, certification of systems, disaster recovery, penetration testing, contingency planning, and security reviews.

Other Executive Branch Agencies (e.g., Department of Interior, National Aeronautics and Space Administration, and Department of Justice) also have budgeted modest amounts for infrastructure protection R&D. Such investments are for internal upgrades and fixes to protect individual agency cyber systems, and as noted in Table 6-3 are not a significant source of R&D funding.

C. THE ROLE OF THE I3P

The foregoing organizations and activities are focused on individual agency's needs and contribute positively to the accomplishment of their R&D requirements. This activity attests to the strength and diversity of current government and private sector efforts to address the national information infrastructure protection problem. However, it

also suggests that some duplication of effort and overlapping of functions is likely. Table 6-4 provides a summary assessment of the adequacy of existing activities to meet key national needs and identifies unmet roles that should be filled by the I3P or other means.

There is a need to create a national perspective on R&D requirements and practices. A number of activities have developed R&D roadmaps, which provide a logical starting point. Current R&D activity needs to be tracked in sufficient scope and detail to identify gaps, shortfalls, and progress and thus establish priorities. These tasks should be assigned to the I3P. The I3P would not actually set the national agenda but would build the information base needed to do so.

Even without a formal national agenda, it is clear that there are critical unmet needs for research in certain areas. As indicated in Table 6-4, these areas tend to fall into the category of basic or fundamental research. There are also unmet needs for research specialized to the designated critical sectors, for example, modeling the sectors and their dependencies and studying cascade effects. Such research is critical to achieving the breakthroughs necessary to protect the information infrastructures over the coming decades, yet funding for basic research is woefully inadequate and likely to remain so without an initiative from the national level.

At the product level, the private sector has primary responsibility. Hundreds of millions of dollars in private R&D are driven by near-term security needs and market opportunities (e.g., new/expanded firewalls, intrusion detection devices, network security software). In certain cases, government-supported organizations should support the development and testing of pre-product prototypes; for example, when private companies under-invest in needed products and technologies due to technical risks or uncertain markets. This is a role that DARPA and NSA have undertaken to meet some of the needs of government users. The I3P also could fill gaps in pre-product development, acting to meet the needs of all the critical infrastructure sectors. Further, the I3P should actively promote the transition of technologies—wherever developed—into the products of the information technology industry.

Table 6-4. Assessment of Existing R&D Activities

Task	Existing Activities	Assessment	I3P Role
Support development and integration of national strategy			
Define and study national information infrastructures as system of systems (interdependencies)	CIAO, aided by Sandia et al. Some sector mapping	Modest start; funding shortfalls Individual sectors only	Perform task across all sectors
Track public and private sector R&D programs to identify gaps, shortfalls, and opportunities	CICG/CIP R&D IWGNCO/CIC for federal programs DoD/NSA/INFOSEC Research Council for selected agencies	Some private sector participation (gaps and shortfalls addressed weakly) Federal R&D only DoD R&D only	Perform task across all sectors
Support development of national R&D agenda for protection of information infrastructures of critical sectors	Roadmap studies for PCCIP	No thorough ongoing effort	Support responsible national or government body
Coordinate and sponsor R&D to fill gaps and shortfalls in key areas			
Establish scientific basis for IA, formal methods and high assurance approaches	Individual agencies and private sector firms each addressing some aspects	Focus on individual agency/company needs; no broad-based national efforts	Selectively fill gaps and shortfalls
Develop engineering principles, standards and metrics for product evaluation benchmarks and tools	NIST, NSA, NIAP Private sector associations/consortia	NIAP R&D budget limited, others tend to concentrate on government needs Limited effort, not always thorough	Selectively fill gaps and shortfalls
Develop systematic methods to analyze cascade effects on interdependent systems	Some sector-specific studies	Methodology and scope limited	Selectively fill gaps and shortfalls
Build modeling and simulation capabilities across key infrastructure sectors	CIAO, aided by DOE labs Private industry by sector needs	Modest start Focus on individual sectors only	Selectively fill gaps and shortfalls
Prototype/test pre-product technologies for end-to-end trustworthy networked systems	Most government and industry entities	No systematic coordination and integration across sectors or agencies (some exceptions in DoD)	Selectively fill gaps and shortfalls
Promote technology transition	CICG CIP R&D IWG DoD (DARPA, NSA, Services)	Results not identified Transfer outside DoD uncertain	Area of emphasis
Develop products	Private industry NSA	Dynamic growth but security inadequate Limited to few government needs	No role

Potential tasks for a new R&D organization are summarized in Table 6-5. These are tasks in which there is a public interest that is not being met by market forces. The topics emphasize basic and specialized research necessary to meet long-term protection needs. The development of specific products, with few exceptions, will be accomplished by the information technology industry.⁴

Table 6-5. Needed R&D Functional Tasks

- Support development and integration of national strategy
 - Define and study national information infrastructures as an end-to-end system of systems in order to understand priorities, linkages, dependencies, vulnerabilities, and risks
 - Track public and private sector R&D programs to identify gaps, shortfalls, and technical opportunities (see information sharing discussion in Chapter VII)
 - Support the development of a national R&D agenda aimed at protecting the information infrastructures of the critical sectors against catastrophic disruptions caused by major, coordinated attacks
 - Sponsor assessments to characterize strategic cyber threats capable of imposing national-level consequences; use classified all-source data from existing intelligence sources
- Coordinate and sponsor R&D to fill gaps and shortfalls in key areas such as:
 - Establishing a scientific basis for information assurance
 - Developing engineering principles, standards, and metrics to provide product evaluation benchmarks and tools (see product evaluation discussion in Chapter VIII)
 - Developing systematic methods to analyze cascade effects on interdependent systems
 - Building needed modeling and simulation capabilities in and across key infrastructure sectors
 - Prototyping and testing pre-product technologies for end-to-end trustworthy networked information systems
 - Promoting the transition of existing and future technologies

D. EXTERNAL RELATIONSHIPS

To perform the tasks described above, the I3P or other organizations would need effective working relationships with a broad set of partners. Part IV below discusses alternative organizational models for accomplishing the R&D tasks. The present section briefly describes the necessary external relationships.

Most importantly, any new R&D organization must work closely with the companies that constitute and operate the critical infrastructure sectors. Ultimately, the

⁴ One exception would be a product needed by the government for which there was insufficient demand to justify commercial development.

protection needs of these companies must define and shape the R&D agenda. Moreover, much of the research outlined above is impossible unless these companies provide sensitive information about their operations and vulnerabilities. The IDA interviews confirmed that these companies hesitate to share such information because its disclosure could damage their reputations or aid attackers in identifying vulnerabilities. They particularly hesitate to share such information with the government for fear that it will lead to increased regulation of their activities.

At the same time, the new R&D organization must work effectively with the government, which is responsible for defining the national security and public safety objectives that would comprise its overarching mission. This requires the trust of the government, which is the primary source of the threat information needed to inform and prioritize the R&D program, and some elements would require access to classified information. Interviews for the present study indicate that the government will be extremely cautious in sharing such information, but detailed access to ongoing government-sponsored R&D projects will be essential for the creation of an R&D agenda.

Finally, a new R&D organization will need to build collaborative relationships with R&D providers such as universities, national laboratories, and the information technology industry. It must work closely with them to track ongoing R&D and support the development of a meaningful national R&D agenda. Moreover, it must be able to bring them together to collaborate in performing needed research. Trust would be especially important in facilitating the transition of technologies into the products of the extremely competitive information technology industry. Research providers contacted during the IDA study expressed a willingness to commit expertise provided that the complicated intellectual property issues involved could be worked out to everyone's satisfaction. Those in the private sector, however, were wary of an expanded government role in conducting, as opposed to sponsoring, research.

Chapter 7

INFORMATION SHARING

Information sharing would be a major activity of the proposed I3P. It is an essential enabler for the organization's other tasks in the R&D, product and services evaluation, and education and training areas as well as an important function in its own right. This function is a valuable service that could increase the effectiveness of all organizations involved in protecting the information systems of the critical infrastructure sectors. What is contemplated here is not an operational role in monitoring computer intrusion and response incidents, a task being addressed by a number of organizations. Rather, the I3P would have a longer-term perspective, concentrating on information needed for study and understanding.

A. NEED FOR INFORMATION SHARING FUNCTION

1. Background

One of the principal observations outlined in the PCAST proposal and validated during our interviews is that R&D information related to protecting the national information infrastructures is not being shared effectively. Although there is a wealth of activity and resultant data available within industry, academia, and government, it is, by and large, not being exchanged within or between those sectors. In consequence, there is duplication of effort in some areas, and little if any effort in other areas. The problem, especially lack of effort, is most pronounced for the area of cross-sector, system-of-systems, cascading effects within complex networks, but it is also apparent for other subjects such as standard setting, best practices, technology transfer, vulnerabilities, threats, countermeasures, security evaluation, training, and policy development.

That information is not being shared is not surprising. Within industry, collaboration is not a natural mode of operations and may violate antitrust laws. Corporations are generally hesitant to share information related to R&D that might be of value to competitors and could threaten market share. Government is hindered because industry is not inclined to provide information regarding security weaknesses for fear it

could result in regulation, investigation, or litigation. And universities, while typically willing to share information, currently have no good forum for doing so; moreover, their information is limited by the fact that information assurance is only now beginning to be treated as a full-fledged academic discipline. Despite these impediments, there is widespread agreement among those interviewed for this study that the security of our national information infrastructure depends on improving the sharing of information.

2. Information Sharing Tasks

The information sharing function would involve a number of tasks, principal among which is creation of a clearinghouse to facilitate the exchange of information among industry, academia and government. This clearinghouse must be perceived as a neutral, non-threatening and secure environment that encourages coordination and cooperation and in which information can be exchanged with freedom and confidence. It would inform researchers of lessons already learned so they could apply those lessons to new research and development. It would provide a place where industries could go to find strategies, policies, and procedures that have been successful in helping other industries defend their infrastructures. Information would be available on these and a variety of other information security subjects, to include threats, vulnerabilities, and countermeasures.

The function would involve active efforts to collect information. The resulting products would be screened and sanitized to ensure that sensitive, proprietary, and classified data is protected. I3P staff would determine the data to be protected, and information would then be organized and stored in a safe repository and made available via secure automated tools in accordance with a well-defined set of rules.

Another task would be to coordinate across sectors and technologies to identify deficiencies and highlight subjects where R&D and other corrective actions are needed. An example might be sponsoring a collaborative analysis of the effects upon the transportation infrastructure of a cyber attack on the telecommunication infrastructure. The goal would be to identify cascading effects and point out to the R&D community where improved tools, policies, procedures, or standards are needed to enhance deterrence, detection, response and recovery. The information sharing function and associated tasks are summarized in table 7-1.

Table 7-1. Needed Information Sharing Functional Tasks

Provide clearinghouse to facilitate two-way sharing of information
Collect, sanitize, analyze, evaluate, archive, and disseminate information
Coordinate across sectors and technologies to identify common deficiencies and highlight areas where R&D or other corrective action is needed

B. EXISTING INFORMATION SHARING ACTIVITIES

Several organizations play a role in information sharing today, and we must determine whether one of them might be able to assume responsibility for the overall function. Principal among them are the National Infrastructure Protection Center (NIPC), the Financial Services Information Sharing and Analysis Center (FS/ISAC), and the National Security Telecommunication Advisory Committee's National Security Information Exchange (NSTAC NSIE). It also should be noted that the Computer Emergency Response Team Coordination Center (CERT/CC) exists for the purpose of sharing information related to infrastructure protection. Its focus, however, is on coordinating immediate response to intrusions and attacks against specific networks rather than on sharing information related to the broader and longer-term aspects of infrastructure protection.

The NIPC is operated by the Federal Bureau of Investigation and staffed by personnel from several federal agencies, including the Department of Defense. While well positioned to deal with federal issues, this is a government organization tied to law enforcement, and industry has reservations about sharing information with such an entity. Also, the government connection may breed fear of regulation and create potential legal issues related to the Freedom of Information Act (FOIA). An additional concern is that the NIPC is primarily oriented toward investigation and operations; that is, solving computer crimes, rather than toward R&D and other aspects of information sharing. Finally there has been little interaction to date between the NIPC and the academic sector.

As envisioned by PDD-63, a single ISAC would be created for the purpose of sharing information among all industries and infrastructures within the private sector. Such a body, if created, would probably be able to perform the function described in this paper; however, efforts thus far to create ISACs have focused entirely on one specific industry or infrastructure. The only ISAC actually established is for financial services (the FS/ISAC). It is operated by a contractor, has limited government and academic involvement, and, having just been activated, has yet to be fully tested. Some discussion

is also taking place regarding a telecommunication and information sector ISAC, but no center has actually been established. There are indications that if one is developed, it might be built upon the existing NSTAC NSIE.

The NSTAC NSIE consists of two subcommittees, one composed of representatives from nine telecommunication and information technology companies, and the other from nine government agencies. The subcommittees hold joint meetings lasting roughly a day and a half every other month to share information on recent intrusions, viruses, and other threats experienced by member organizations. The NSIE does provide a forum for sharing information among industry and government, and to a certain extent academia. (The CERT/CC, associated with the Software Engineering Institute (SEI) at Carnegie-Mellon University, attends as a guest). However, its effectiveness in performing the overall function would probably be limited by the fact that it is not a standing organization staffed by a significant number of full-time personnel. In addition, its focus is rather narrow, concentrating on operational response to threats, and vulnerabilities to individual member companies and agencies.¹

As indicated in the foregoing discussion, while there are several organizations that perform various aspects of information sharing, none seems suitable for performing all the tasks outlined above. Our findings, summarized in Table 7-2, lead us to conclude that a new entity is needed—one that takes an overarching view, looking across sectors and technologies and concentrating on R&D, system-of-systems effects, and broader aspects of information assurance such as policy development.

¹ The NSTAC itself has conducted a number of broader studies of the vulnerabilities of particular infrastructure sectors.

Table 7-2. Assessment of Existing Information Sharing Activities

Task	Existing Activities	Assessment	I3P Role
Provide clearinghouse and facilitate sharing of information among industry, academia, and government	NIPC	Government agency closely connected with law enforcement. Industry may not be inclined to share information. Focuses on operations versus R&D. Little academic involvement.	Provide a neutral, non-threatening venue. Facilitate coordination and communication across and within sectors.
	FS/ISAC	Focuses on financial services sector only. Limited government and academic involvement.	
	NSTAC NSIE	Shares information but focuses on operational response versus R&D. Meets only periodically. Limited academic involvement.	
	CERT/CC	FFRDC, but private institution; info exchange for government, industry, and academia	
Collect, sanitize, analyze, evaluate, archive, and disseminate information	NIPC	Limited ability to collect information from private sector. Focus is on operations versus R&D.	Conduct active information gathering; consolidate into library and databases; disseminate information; protect sensitive information and sources.
	FS/ISAC	Only handles information within sector. Not connected with government. Newly formed; effectiveness not determined.	
	NSTAC NSIE	Collects and archives very limited amount of information. Not staffed for analysis and evaluation.	
	CERT/CC	Focus on coordinating response and disseminating information related to computer intrusion rather than on R&D.	

Continued

Table 7-2. Assessment of Existing Information Sharing Activities (Cont'd)

Coordinate across sectors and technologies to identify common deficiencies and highlight areas where R&D and other corrective action is needed	NIPC	Limited ability to collect information from and engage private sector in collaborative effort.	Sponsor collaborative analysis of deficiencies across industries. Bring findings to attention of R&D and other organizations.
	FS/ISAC	Focused only on financial sector.	
	NSTAC NSIE	Focuses on specific threats and vulnerabilities of member companies and agencies.	
	CERT/CC	Closely associated with SEI but does not work in R&D field	

C. THE ROLE OF THE I3P

The principal role of such a body would be to provide linkages among industry, academia and government to facilitate two-way sharing of information. This would involve building strong relationships and encouraging communication, cooperation and coordination among those sectors. It could be accomplished by creating a neutral, non-threatening, mutually supportive organization which would, among other things, sponsor workshops, symposia and other forums and produce publications for the purpose of apprising members of one sector on activities in the other sectors. The organization would act as a central source, in essence, a clearinghouse for information.

One significant task in accomplishing the function would be to actively collect information on activities within government, industry, academia, and from foreign sources. All traditional information gathering techniques would be employed, to include web and literature searches, interviews and professional gatherings. Specific emphasis should be placed on acquiring information related to the functions of R&D, product and service evaluation, and training and education, although all topics related to information infrastructure protection would be of interest. Within the area of R&D, information should be obtained pertaining to current projects and their participants, goals, tools, methodologies, and results. Particular attention should be paid to projects that address cross-sector, system-of-system effects. In addition, information should be gathered on policies, laws, and standards and how they affect the information infrastructure. Other aspects of information assurance, such as threats, vulnerabilities and countermeasures, should also be pursued.

The I3P would need to be especially careful in handling data and scrupulous in its sanitization efforts. It must be acutely aware of the sensitive nature of much of the information and must be able to guarantee the confidentiality of its sources. The organization should also have classification authority and a well-documented set of procedures for dealing with proprietary and classified information. Binding non-disclosure agreements and government security clearances would probably be required.

The I3P would need to be populated with respected experts who could analyze and evaluate the raw information collected. With its broad view across sectors and technologies, the group would examine information, looking for common threads and patterns. It might, for example, look for the most pervasive vulnerabilities, or those vulnerabilities having the greatest consequences, to suggest areas in which R&D efforts should be focused.

The I3P would build and maintain a repository of information. This would involve integrating, organizing, and archiving information. It would include developing and maintaining databases, catalogues and baselines, including a list of subject-matter experts and a lessons-learned library.

Coordination among participants should be continuous. This would require a means of secure and efficient communications, ideally a collaborative tool that employs web technology to facilitate information dissemination, assign and track projects, monitor program events and schedules, provide e-mail notification when new information becomes available, and offer access and search capabilities for the information repository.

D. EXTERNAL RELATIONSHIPS

The I3P must establish liaison with, track the activities of, and gather information from external organizations performing related work. This is essential to avoid duplication and conflict and to optimize efforts. External groups of primary interest include the NIPC and others discussed above as well as the following:

- Industry consortia, associations, and committees, such as
 - Information Technology Association of America (ITAA)
 - Telecommunications Industry Association (TIA)
 - U.S. Telephone Association (USTA)
 - Electric Power Research Institute (EPRI)

- National security committees, including
 - National Security Telecommunications and Information System Security Committee (NSTISSC)
 - National Communications System (NCS) Communications Resource Information Sharing (CRIS) organization
- University research organizations
- National Academy of Sciences
- Government research organizations, including
 - National and DoD Labs
 - National Security Agency
 - Defense Advanced Research Projects Agency
 - National Science Foundation
 - National Institute of Standards and Technology
 - National Coordination Office for Computing, Information and Communications
 - Information Assurance Technology Analysis Center
 - CERT/CC Coordination Center and other computer emergency response teams

As indicated at the beginning of this chapter, while there is a wealth of activity related to protecting the information infrastructure, there is a significant shortcoming in the sharing of relevant information. As a result, efforts are largely uncoordinated and do not address critically important cross-sector concerns. Furthermore, while a number of existing organizations are involved in information sharing to some extent, none is performing all necessary tasks. In conclusion, then, a new entity is needed, one that has broad perspective, excellent professional credibility, well-established ties with all sectors, and the integrity to respect the confidentiality of sensitive information. It is envisioned that the I3P, properly designed and staffed, would be able to fill this role.

Chapter 8

PRODUCT AND SERVICES EVALUATION

Evaluating products and services would be a principal subject area addressed by the I3P. The goal would be to identify, support, and recommend evaluation services that meet the needs of critical infrastructure sectors. For the most part, evaluation services themselves would be performed by organizations other than the I3P. As discussed in the previous two chapters, this subject area would include important R&D and information sharing activities.

Terminology in this area is fluid but it is important to distinguish certain concepts. The words "testing" and "evaluating" will be used interchangeably in this chapter to denote the basic activity of testing a product or service against specified evaluation criteria, which may be based on formal standards, accepted benchmarks, or ad hoc specifications. A distinct activity, validation or certification of the test results may raise credibility if done by an authoritative third party. Another credibility-enhancing activity is the accreditation or certification of the testing organization or its professionals. In practice, many if not most evaluations are performed by unaccredited organizations and the results are not separately validated.

In the following discussion, terms such as "standard," "benchmark," and "best practice" are used to describe variants of the concept, "this is ok." Generally, "standard," at the beginning of the list, connotes the most formality and implies something obligatory, whether government-specified or market-driven or voluntary. At the other end, "best practice" connotes informal information, the use of which is discretionary; that is, it is not really a standard at all. The discussion also encompasses the different "branches" of information assurance, including both security products and the security aspects of (a) broader-purpose information technology products and (b) systems and networks, both new and deployed. We also address professional services organizations, information assurance professionals, and information assurance education.

A. NEED FOR PRODUCT AND SERVICES EVALUATION FUNCTION

Available evaluation services are generally viewed as inadequate to meet the needs of the critical infrastructures. The people interviewed by IDA generally support measures to improve these services. However, there is no consensus on what should be done to develop better standards to support more effective evaluations.

1. PCAST Proposal

The PCAST proposed a technical program that would include work in component and software security assurance, including developing best practices for product evaluation. The PCAST also proposed programs that would provide a linkage between government and industry and draw upon talent in academia for the purposes, among others, of setting and disseminating best practice information and carrying out training exercises and inspections to certify performance.

2. Phase 1 Results

In IDA's Phase 1 interviews and workshop, there were a significant number of suggestions to the effect that new or strengthened functions are needed in evaluating products and services, including expanded tests, exercises, and inspections to certify performance. The notion of an "Underwriters Laboratories (UL®)" for trustworthiness came up on a number of occasions. The need for interoperability standards and more generally for standards for trustworthiness in information systems operations and management was suggested by some interviewees. Thus the Phase 1 results reinforced the general thrust of the PCAST recommendations in the area of product and services evaluation.

3. Phase 2 Results

In Phase 2, a working group made up of IDA staff and consultants, assisted by comments from a dozen industry, academic and government practitioners, prepared for what proved to be a lively discussion of product and services evaluation and standards setting in a workshop held in September 1999. A comprehensive set of desirable criteria for a product and services evaluator, developed by the Phase 2 working group, is provided on Table 8-1.

Table 8-1. Desiderata for a Product and Service Evaluator

- A. Applies standards that are from recognized standards organizations or self-developed using credible and appropriate processes. Because of the pace of change in information technology, evaluation may well occur long before formal standards can be agreed to and issued. Therefore, test methods and criteria are often created *ad hoc* by the evaluator and/or vendors; in such cases a credible process is needed that reflects the interests of the end users and not just the vendors.
- B. Operates "transparently" Processes, procedures—and perhaps some or all test results—are available for independent review. This does not mean the evaluator should broadcast the fact that a product or service fails or the reason it fails. Also, as addressed below, proprietary information must be protected. The underlying goal is that users and vendors have confidence in the evaluator's processes and results.
- C. Is financially and organizationally independent from vendors whose products and services are evaluated. It may not be feasible for the evaluator to be completely independent in this sense. Complete financial independence ("we accept no advertising...") is important in the consumer environment, but less so in a business-to-business context. The government, as a customer, has been willing to pay for product certification. Commercial customers have expected vendors to pay to have their products evaluated by a third party that is *organizationally* independent from the vendors. Organizational independence includes the concept that there must be protection from political interference of various kinds. Political considerations should not affect the evaluator's processes or threaten its funding or continued existence.
- D. Is objective Objectivity may, in fact, be more important than independence. At minimum, if there are biases or conflicts of interest, they must be identified and disclosed. Beyond this, what makes an evaluator non-objective and what constitutes a conflict of interest is less clear. Some product evaluators claim objectivity since they (and their affiliated companies) do not make the kinds of products being evaluated. However, they may provide security consultant services or publish trade magazines. At the same time they have to maintain a reputation for objectivity in order to sell their certification service. Therefore, what assurances of objectivity will be required to engender trust of the evaluator among both customers and vendors remains unclear.
- E. Is well qualified This is generally concluded based on the evaluator being accredited by an oversight entity. In the case of NIAP, described in Section B1 of this chapter, this is augmented by having a second entity validate the evaluator's work.
- F. Protects sensitive proprietary information Appropriate protections must be in place and respected. The evaluator should have clear-cut and well defined practices that are available to developers and users. Protections must be strictly applied and breaches—should they ever happen—should be dealt with openly. Moreover, the "supplier" community must be comfortable with the organization and its information protection arrangements. This could be difficult. Not only must the organization be trusted, but the evaluator's employees may be subject to restrictions on future employment because of their access to such information. Access to "the best and the brightest" may suffer.
- G. Has the respect of the relevant community Both customers and vendors must be willing to entrust evaluation to the evaluator and to accept its methods and conclusions. This respect will probably come from the evaluator having all of the necessary characteristics discussed here. The evaluator may be a government organization if and only if all other characteristics are assured; freedom from political interference and independent funding may be the stumbling blocks here.
- H. Role must be appropriate to the organization's mission A multi-functional organization can perform evaluations if that is consistent with the other parts of its mission. An organization whose only function is to evaluate may be preferable.

The product and services evaluation function turned out to be quite complex. It would be wrong to say we have detailed knowledge of what is going on across all branches of information assurance and all infrastructure sectors. We know enough to say for sure that activity is very uneven, and more to the point, to say that no one has a clear picture of the totality of on-going and planned activities. In 1999 the evaluation and

standards setting area was a fermenting pot. However, in the course of this work, it became clear that the functions I3P would perform in this area were quite circumscribed, perhaps best summarized as harmonizing, facilitating, and gap filling.

There was no dissent to the view that testing and evaluation are appropriate functions to be performed across all branches of information assurance and all infrastructure sectors. However, evaluations necessarily involve using test criteria of some kind and the proper nature and source of these criteria are not generally agreed. In particular, there is no consensus that formal standards are required. A general standard, the "Common Criteria" (ISO/IEC 15408), has been developed to guide the definition and testing of security requirements. This has been a government-led effort, and it remains to be seen how widely it will be accepted for commercial evaluations. Perhaps even more controversial is the need to develop formal standards to serve as test criteria for particular types of products.

Attitudes toward standards vary greatly, for example, among the three communities of information technology users, vendors, and researchers. Users, including some infrastructure operators, would like to procure products that are certified (e.g., a shrink-wrapped box with a UL® mark) to conform to standards that virtually guarantee security, reliability, safety, etc. Relatively few users realize that they must take responsibility for understanding the information that a product evaluation conveys as to the standards applied and the qualifications of the evaluator. Vendors, too, have varied attitudes, depending on how standards would affect their businesses. Most express a preference for no standards at all. Some hope to dominate market segments by establishing their proprietary designs as de facto market standards they can license or deny to other vendors. Some view standards, whether formal or not, as a means of constraining other vendors, for example, to ensure interoperability and markets for their niche products.¹ There are also concerns about national standards—as opposed to international standards—serving as non-tariff barriers and restricting international trade. Vendors facing the possibility of multiple standards clearly prefer a single standard for a

¹ The interoperability of security products is part of a larger interoperability issue. Often, vendors dominating a particular market segment do not want to be interoperable. For example, during the time of this study (summer and fall of 1999) AOL and Microsoft were battling over instant messaging protocols. Reportedly, Microsoft had changed its messaging software more than a dozen times between June and September 1999 to exploit "back doors" in AOL's system as AOL sought repeatedly to prevent the 2 million users of Microsoft's network from sending instant messages to the 17 million AOL users. An ad hoc open standard working group was meeting to develop something in 1999 that would allow open instant messaging among Internet service providers, notably AOL and Microsoft.

type of product, thereby avoiding the complications of meeting different standards for different sectors. More than most people, academics and research scientists realize that fundamental questions remain to be answered before solutions can be promulgated on which broadly applicable—and, especially, quantitative—standards can be based for testing products, systems, and networks. Such professionals—those in academia more than those in private or government research establishments—are constitutionally averse to piecemeal solutions of any sort, standards to address this or that specific interoperability problem included. Finally, researchers are especially sensitive to the fact that information technology may develop in a quite unexpected direction at any time. To be able to respond to the unexpected, they would very much prefer to do their research without being encumbered by any limitation.

Virtually all parties in the private sector share an aversion to government involvement in their businesses. The evidence collected in this study suggests that government involvement in standards setting is often viewed as too close to government regulation for comfort. In sum, efforts to develop standards are highly controversial and there is no consensus on what more should be done in this area. However, there is a recognition that gathering and disseminating information on best practices is a useful function. There is a clear need to look across the activities, for example, of states that license information assurance professionals, academic accreditation bodies, and various product, system and network evaluators to share knowledge on “what works” and point out inconsistencies, especially those that have the potential for creating vulnerabilities.

B. EXISTING ACTIVITIES

Product and services evaluation spans a wide range of activities involving many different organizations. A number of important activities and organizations are only now emerging, thanks to the increasing concern for information assurance. This section provides concrete examples of the work that is being done.

1. U.S. Government

The most stringent product evaluation program has been operated by the Defense Department’s National Security Agency (NSA). Under its Trusted Product Evaluation Program (TPEP), NSA previously conducted all trusted product evaluations in-house. Under a more recent program, the Trust Technology Assessment Program (TTAP), NSA allows designated commercial laboratories to evaluate products at specified levels of

trust. NSA validates each evaluation and publishes an Evaluated Products List. NSA focuses on products needed by the government, although commercial users may find the results useful. The evaluation and validation process is funded by the government and, in some cases, by vendors.

The Commerce Department's National Institute of Standards and Technology (NIST) oversees testing of information technology products for conformance with Federal Information Processing Standards (FIPS). For example, NIST allows certain commercial labs to test cryptographic modules for conformance with FIPS 140-1. NIST itself then validates the test results. These tests are funded by the government for the benefit of government users.

The National Information Assurance Partnership (NIAP) is a joint effort begun in 1997 by NSA and NIST to develop the capabilities of commercial test laboratories to evaluate products based on the Common Criteria (ISO/IEC 15408).² NIST's National Voluntary Laboratory Accreditation Program (NVLAP) is currently in the process of accrediting the first group of labs, based on criteria defined by NIAP. Once product evaluations begin, NIAP will validate the results³ and publish a validated products list. Product evaluations will be funded primarily by product developers and vendors, although NIAP may also provide financial support in some cases.

NIAP currently views virtually any information technology product as "potentially useful to the government" and therefore acceptable for validation. Vendors or other evaluation sponsors will contract with and pay NIAP-approved laboratories to perform evaluations. The sponsors will decide whether to seek validation of the results by NIAP or some authority other than NIAP, or to forgo validation, relying on NIAP approval of the laboratories as sufficient assurance. NIAP's status as a government entity is likely to attract some sponsors and repel others. A potential advantage of NIAP validation is the "Mutual Recognition Arrangement" under which the U.S., Canada, and several European governments have agreed to recognize each other's Common Criteria validations. In

² NSA's own evaluation programs are also based on the new Common Criteria. Previously, they were based on the Trusted Computer System Evaluation Criteria, known as the "Orange Book."

³ This practice—validating the results of individual tests performed by others—is used by NSA, NIST, and certain foreign governments. It enables government agencies to shift testing to the private sector yet still meet their responsibilities as approval authorities. This approach may prove useful in certain commercial niches where security requirements are particularly high. In other cases, however, selecting accredited testers whose performance is monitored by their accreditors may prove to be a sufficient—and far less costly—means of gaining assurance of the validity of test results.

effect, NIAP validation will place a product on an international validated products list, enabling a vendor to sell to any of the participating governments without further testing.

In the future, NIAP plans to address deployed systems as well. NIAP will define criteria for evaluating such systems and for the accreditation of organizations to conduct evaluations. NIAP will validate the results. NIAP also has a research mission—not, at this time, well funded—to develop test methods and tools.

2. BITS Laboratory

The Banking Industry Technology Secretariat (BITS), under the Financial Services Roundtable, established the BITS Financial Services Security Laboratory in the summer of 1999. This new “BITS Lab” illustrates the concepts of sector specialization and user control. BITS Lab will specialize in evaluating products of interest to the financial services industry, including both security products and the security aspects of e-commerce products. It will be a “self-validating” organization, awarding a “BITS Tested Mark” to products that pass its tests. Financial companies will be encouraged to give preference to such products. While specialization offers potential economies in evaluating sector-specific products, it could also lead to wasteful duplication and increased costs per test if each sector insists on its own evaluation of common generic products. These are moot points for the financial sector since, until NIAP is operational, there are no viable alternatives for thorough commercial evaluations.⁴

Perhaps more important to users in the financial sector is the control BITS Lab gives them over the evaluation process. BITS Lab will be operated under contract by Global Integrity, a subsidiary of Science Applications International Corporation (SAIC). A Laboratory Governance Committee of security professionals will establish priorities and security requirements for each product class, drawing on a master set of relevant standards from ANSI, ISO (including the Common Criteria), federal regulators, and other sources. Global Integrity and the product vendors will develop test plans for specific products. Thus, even though vendors will be “funding members” of BITS Lab and will pay for product testing, BITS Lab will ensure that the process serves the interests of

⁴ The NIAP model will also accommodate sector-specific products. For example, NIAP is defining formal Common Criteria security requirements (called Protection Profiles) for a number of specialized products, including Smart Cards and telephone switches. If necessary, NIAP will also develop specialized test methods and criteria for accrediting specialized labs. BITS Lab itself might seek accreditation as a Common Criteria lab.

financial sector end users.⁵ The financial sector, valuing flexibility and responsiveness, may also count independence from government processes as an advantage.

It is unclear whether other sectors will establish their own evaluation processes. Coordination of such processes across sectors to avoid conflicts and unnecessary differentiation (see Section C1 below) could be a potential role for the I3P.

3. Commercial Evaluation Services

A broad range of commercial evaluation services is available. Information technology vendors can pay consultants or independent labs to evaluate their products and attest to their findings. A few organizations are trying to establish themselves as self-validating authorities, evaluating products and awarding widely recognized certification marks. Examples include ICSA, Inc. (referred to as International Computer Security Association) and West Coast Labs. ICSA, for instance, organizes consortia of vendors to develop test criteria for products such as firewalls and anti-virus software. Vendors pay ICSA to have their products tested and those that pass are awarded the ICSA certification mark. The tests are "black box" evaluations, focusing on specified performance features, such as the ability to identify and defeat a list of potential attacks.⁶ Such tests are valued for their speed and low cost, but they lack the thoroughness of Common Criteria tests, which also address such matters as how a product is developed and how it functions internally. To build a respected certification mark, ICSA must maintain a reputation for objectivity and integrity. However, it is clearly providing a service for vendors; end users apparently do not directly influence the evaluation process.

Buyers guides for generic information assurance products offer another useful service. For example, *PC World* from time to time publishes comparisons of the leading anti-virus software products. Comparisons are based on black box performance tests, useful features, and prices. A tutorial on product functions is included. While such comparisons provide information not conveyed by a pass/fail certification mark, the

⁵ For example, test criteria will be based on the needs of the financial sector rather than a lowest-common-denominator consensus among information technology vendors.

⁶ Tests for anti-virus products, for example, are based in part on the Wild List, which identifies viruses that are known to be infecting computers (as opposed to viruses that exist only in computer labs).

information is time-limited. The buyers guide approach does not lend itself to ensuring that a product continues to meet requirements as time passes, often an essential feature of a security product.⁷

4. Evaluating Deployed Systems

Security evaluation of the operational cyber systems of the critical infrastructure sectors is essential. Such evaluations should examine whether security policies are adequate and enforced, whether system architectures provide adequate protection (including redundancy, fault tolerance, and security), and whether security components are configured and operated correctly. Red-teaming (staged cyber attacks to uncover vulnerabilities) can be very useful evaluation tools.

In the private sector, a wide variety of consultants offer network security services, including assessment and remedial advice. The providers range from well known companies such as Ernst & Young, which offers a service called eSecurity Solutions, to small startups whose competence is unknown. ICSA offers a structured approach for user networks connected to the Internet called TruSecure, which includes assessment and advice on improving security. ICSA awards TruSecure certification to qualifying systems, conducts follow-up audits and spot checks, and requires annual re-certification.

Many large organizations perform their own system evaluations. The Department of Defense (DOD), for example, requires a "certification and accreditation" process for all of its operational information systems.⁸ For each system, a Certification Authority is appointed to evaluate whether system-specific security requirements are satisfied. A Designated Approving Authority for that system then accredits (i.e., authorizes) its operation if it can be operated at an acceptable level of risk given its mission. While DOD attempts to identify classes of systems with similar security requirements, it has not

⁷ To retain an ICSA certification, for example, a vendor must make a contractual commitment to meet published criteria. For anti-virus products, the criteria are updated monthly to reflect new threats. ICSA spot checks products two to four times per year, insists on needed corrective action within seven days, and requires annual recertification. Non-complying products are removed from the certified products list. Under the NIAP scheme, a validation certificate applies only to the specific product version/release that is evaluated. However, by complying with a Certificate Maintenance Program, a sponsor can obtain updated validation certificates for modified products without repeating the full evaluation process. A NIAP-validated plan must specify ongoing maintenance activities, required evidence of compliance, what must be verified by the testing lab, and what circumstances would make a full re-evaluation necessary. Among other things, changes in the threat environment may be considered.

⁸ The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is defined in DoD Instruction 5200.40, December 30, 1997.

defined system security standards. Ultimately, authorization to operate depends on the informed judgement of a designated authority.

Overall, the evaluation of deployed systems is hindered by a lack of evaluation standards and by the absence of an authoritative entity to accredit the organizations that conduct evaluations and, in certain cases, validate individual evaluations. As noted above, NIAP intends to address these needs, but many people question its future because of the prevalence in industry of antipathy to involving a government entity in internal operating matters.. This area is very important for the critical infrastructure providers, who need assurance that their own systems are secure. Further, they need an efficient and authoritative means of determining whether interconnected systems owned by other companies are secure.

5. Professional Certification

Perhaps a prerequisite for improving the evaluation of deployed systems is building a corps of recognized, credible security professionals. At least two national organizations offer relevant certification programs. The International Information Systems Security Certification Consortium (ISC)² awards the Certified Information Systems Security Practitioner (CISSP) designation. Qualifications include gaining information assurance experience, complying with a professional code of ethics, and passing a test on the relevant common body of knowledge. Re-certification is required every 3 years and reflects interim activities. The Information Systems Audit and Control Association (ISACA) administers the Certified Information Systems Auditor (CISA) designation held by more than 12,000 professionals worldwide. There are also state-level programs that may affect security, for example, the licensing of software engineers by the State of Texas. However, judging from the comments of industrial participants in the IDA working groups, it is not clear that these programs have had a perceptible impact in industry.

6. Standards Organizations

As is evident from the discussion above, many organizations are involved in establishing benchmarks, criteria, and standards for testing and evaluation in the various branches of information assurance. The confusion evident in these processes is relieved only somewhat by the existence of a recognized formal worldwide system for standards setting.

At the top of the international hierarchy of information technology standards setting entities is the Joint Technical Committee 1 of the International Standards Organization and the International Electrotechnical Commission. Standards for information assurance are the purview of Subcommittee 27 (ISO/IEC JTC1/SC27), which has emphasized cryptology but lists international standard ISO/IEC 15408 (Common Criteria) among its products. ISO/IEC JTC1 members are a mix of national government and industry-supported organizations.

The American National Standards Institute (ANSI) is the U.S. member of ISO/IEC JTC1. In principle, ANSI could carry out "conformity assessment" activities, such as accrediting third party product certifiers in the area of information assurance. However, in practice, this is being done under the NIAP Common Criteria scheme.

Specialist industry and professional groups also establish standards within the ISO/IEC system and on their own. For example, the Institute of Electrical and Electronics Engineers (IEEE) is an ANSI "accredited" standards development organization. The IEEE Computer Society is the largest of the IEEE societies and is responsible for standards development (including those pertaining to security), a process that is inclusive in participation and elaborate procedurally, reflecting ISO and ANSI policies. Once approved internally, IEEE standards are usually provided to ANSI and ISO and other national, regional and international organizations for possible adoption.

To carry the example a step farther, the IEEE Computer Society Internet Best Practices Standards Working Group has been addressing Internet security recommended practices, building on the work of the Internet Engineering Task Force (IETF) and the Web Consortium, among others. The IETF and Internet Engineering Steering Group (IESG), related to the Internet Society (INSOC) and the World Wide Web Consortium (W3C), develop standards for worldwide web security through the IETF Security Area Advisory Group (IETF/SAAG).

In addition to those named above, other industry and professional groups carry on what is in effect standards development work. The Association for Computing Machinery (ACM) Special Interest Group on Security, Audit and Control (ACM/SIGSAC) sponsors conferences and workshops, and publishes transactions, that establish the groundwork for standards. There is an IEEE Computing Society and ACM Software Engineering Coordinating Committee, which, among other things, is developing a "Guide to the Software Engineering Body of Knowledge" for use in licensing and certification of professionals. It is not focused on security matters.

Other membership organizations participate in the area of information assurance. Almost always they are related by interlocking directorates and cooperative agreements. In some cases there is a well-established hierarchy for standards setting. However, the processes are complex at best and work slowly. Fragmented organizational arrangements and convoluted processes in standards setting are part of the reason that standards setting cannot keep up with the pace of information technology development.

7. Assessment of Existing Activities

The sections above portray the highlights of activities in the area of product and services evaluation. While a great deal of work is being done, important gaps exist and some key activities are new and untested. Table 8-2 identifies key evaluation-related tasks and organizations and offers summary assessments of whether existing activities are adequate to perform the listed tasks.

Evaluation capabilities currently appear to be more advanced for products than for deployed systems. While thorough and authoritative commercial product evaluations are not readily available today, paths forward have been identified, some umbrella standards have been defined, and organizations are being established, with NIAP as the most prominent. It remains to be seen how successful these efforts will be and, in particular, how well they will meet the specialized needs of the critical infrastructure sectors. For deployed systems, in contrast, the way forward is not apparent. NIAP might fill the organizational gap, but it will take an enormous effort to develop generally accepted standards, evaluation criteria, and test methods. In fact, the general area of providing tools and support for the evaluation of both products and deployed systems requires greater attention. The potential role of I3P in addressing current gaps and weaknesses is discussed in the following section.

Table 8-2. Assessment of Existing Product and Services Evaluation Activities

Task	Existing Activities	Assessment	I3P's Role
Product Evaluation			
Accredit test labs	--NIST's NVLAP for NIAP	Too soon to judge	
Test/evaluate products	--NSA, thorough, limited --NIAP, thorough but new --BITS, for bank sector, new --ICSA, WCL, black box testing	Many new initiatives, too soon to judge	
Certify/validate tests	--NSA, own and outside tests --NIAP, outside tests --NIST, outside tests --ICSA, WCL, own tests	Many new initiatives, too soon to judge	Potential niche validator
Prepare buyers guides	--Trade press, black box snapshot --Associations, technical tutorial	Coverage emphasizes mature products	
Deployed Systems Evaluation			
Accredit testing organizations	--NVLAP, proposed for future	No existing activity	Potential niche accreditor
Test/evaluate systems	--NSA, NIST for federal systems --Consultants, range of services --Self test, informed entities	Competence uneven, methods ad hoc	
Certify/validate tests	--NIAP, proposed for future	No existing activity	Potential niche validator
Tools and Support			
Develop testing methods, tools, metrics	--NSA, has expertise --NIAP, mission underfunded	Focus on government needs, funding inadequate	R&D, info sharing, tech transfer
Develop test and accreditation criteria	--NIAP, based on CC --BITS, based on mix --ICSA, by vendor consortia	Need to define and harmonize specific criteria	R&D, info sharing
Develop product and interoperability standards	--IEEE Computer Society --IETF, for interoperability --ANSI, IOC, IES --NIST for government FIPS --Associations, specific interests	Multiple channels and slow processes	Info sharing, perhaps facilitate
Maintain attack databases	--Wild List, relevant viruses --Testers, relevant threats --Manufacturers, relevant threats	Some information closely held for market advantage	Info sharing
Maintain IA test bed	--Consultants, for general IT --Government (NRL, DARPA)	Gaps in special-purpose facilities	If needed for R&D function
People and Training			
Accredit IA curricula and schools	--CSAB, computer science --SECC, software engineering	No IA focus at this time	Info sharing, encourage accreditors
Accredit IA professionals	--(ISC) ² , info security --ISACA, info system audit	Emerging, relevant programs	Info sharing

C. THE ROLE OF THE I3P

The critical infrastructure providers must first have available products and services to protect their infrastructures and must then have access to and utilize efficient evaluation services. Such services are essential for building, operating, and interconnecting secure systems, and promoting them should be a major concern of the I3P. However, the I3P should play a supporting role, harmonizing, facilitating, and gap filling, but relying on other organizations for operational activities. The I3P's R&D and information sharing activities should prove particularly useful in the evaluation area. Table 8-3 summarizes these roles, which are discussed in succeeding sections.

Table 8-3. Needed Product and Services Evaluation Functional Tasks

- | |
|---|
| <ul style="list-style-type: none">• Promote the establishment and use of evaluation services that meet the needs of the critical infrastructure sectors<ul style="list-style-type: none">– Harmonize processes and criteria used by overseers and evaluators– Facilitate on-going work and the establishment of new capabilities, as needed– Fill gaps in evaluation and standards area where only the I3P is serviceable• Oversee an R&D program to improve test methods and develop tools, metrics, and benchmarks (see Chapter VI on R&D function)• Establish and maintain linkages that promote the gathering and sharing of information on best practices among testers, vendors, researchers, and infrastructure operators (see Chapter VII on information sharing function). |
|---|

1. Harmonize Processes and Criteria Used by Overseers and Evaluators

The I3P would have a broad perspective encompassing all of the critical infrastructures and the various branches of information assurance. It would thus be well positioned to promote a voluntary convergence of evaluation processes and criteria. Harmonization could strengthen the evaluation area by promoting wide use of best practices. Further, it is important to avoid a willy-nilly proliferation of evaluation organizations and criteria. Such differentiation can raise costs by splitting markets or forcing multiple testing of individual products. It can also weaken the recognition and authority of the various processes. Differentiation that does not serve a necessary purpose should thus be avoided.

It remains to be seen how much differentiation will be necessary to meet the specific needs of various critical infrastructure sectors. The sectors rely on a mix of sector-specific and generic hardware and software products, and there are important differences in the vulnerabilities of their critical cyber systems. Some sectoral

specialization may thus prove advantageous, either within a broad approach such as NIAP or through sector-specific organizations such as BITS Lab.⁹

The degree to which the I3P should become involved in establishing benchmarks, criteria, or even standards is unclear. Certainly, taking broad responsibility for standards setting would encroach on the responsibilities of other organizations. Further, it would risk alienating industry, whose cooperation is essential, because industry tends to see government involvement in creating standards as the initial step on a slippery slope toward government regulation. In addition, it would place at risk the cooperation of those researchers who believe that standard setting is premature for the foreseeable future.¹⁰

2. Facilitate Ongoing Work and Establishing New Capabilities, as Needed

From time to time, as the I3P promotes the availability of needed evaluation services, it will identify opportunities to make useful contributions. These likely will be very focused, finite activities to facilitate on-going work or jump-start new projects. In such cases, the I3P should be able quickly to provide modest funding (e.g., $\leq \$100,000$) and temporary staffing to seed selected new initiatives or free up work stuck at a critical juncture. An example might be bringing the protagonists in an important interoperability dispute to the table to settle on an appropriate interoperability standard.

3. Fill Gaps in Evaluation and Standards Area Where Only the I3P Is Serviceable

Overall, the I3P could serve best by not being directly involved in the day-to-day processes of evaluation and standards development. It should be quite enough that it gathers information on best practices to support its own scientific and policy research function, and incidentally disseminates this information widely. If the need for a new evaluator or overseer or a new standard-setting process arose, I3P should prefer to use its facilitation capabilities to help stand up an appropriate entity. However, it is possible that a unique circumstance would arise in which it made sense for the I3P to be an overseer in a very specialized niche. For example, for deployed systems, it might be needed as the

⁹ Also, there are inherent testing tradeoffs between thoroughness on the one hand and cost and speed on the other. Differentiation may thus be necessary to accommodate the tradeoff preferences of various market segments.

¹⁰ Some interviewees thought that more sophisticated testing and standards were futile. Until users take reasonable advantage of what is available to them now, in this view, procedural and measurement refinements are a waste of resources.

authority for accrediting evaluators or possibly even validating individual evaluations, particularly if unique system-of-systems properties are at issue.

However, two principles are clear: I3P should never compete with an evaluator or overseer that is working at all satisfactorily, and it should not aspire to a broad function as an overseer or evaluator. It nonetheless seems sensible to avoid hard and fast decisions on such possibilities in advance because a very large question looms over the evaluation business. Will NIAP succeed? Some interviewees said that it will not be able to throw off the habits that have made past government evaluations costly, slow, and risky to the vendor. Also, government validation of individual test laboratory evaluations is a potential bottleneck. Even more basic, many believe that an evaluation regime created and controlled by the U.S. government is suspect, no matter how hard it works to show absolute objectivity. They hold that the government is necessarily schizophrenic in its approach to information assurance. Some parts of the government want to enhance security; others want to monitor, measure, and penetrate transmissions and computers. There is a significant market segment that will always believe a government validation of a security product or system means a "back door," known only to NSA, has been built into it.

The jury is still out on NIAP. Should the I3P be positioned to fill in if NIAP proves to be unacceptable because of its status as a government agency? The answer is not clear, partly because it will depend on the final shape of the I3P. If the problem is distrust of government mechanisms, the I3P must be sufficiently distant from government control so as to be quite independent, both at first glance and after detailed scrutiny.

4. Oversee an R&D Program to Improve Test Methods and Develop Tools, Metrics, and Benchmarks

Identifying basic research needs would be a principal value of the I3P's activities in the evaluation area. At present, the absence of a scientific basis adequate to establish sound test criteria, let alone broadly applicable standards, greatly limits the effectiveness of evaluations. A major product of gathering and sharing information on best practices would be the identification of gaps in the scientific knowledge base that supports the evaluation of products and services.¹¹ This, in turn, would guide the I3P's scientific

¹¹ The seminal 1999 book, *Trust in Cyberspace*, pointed out that there is no way to test large-scale systems. It suggested research emphasizing risk mitigation as opposed to risk avoidance, for example, to limit the magnitude of the propagation of outages. It also noted that interfaces are an important area

research program. Tests different than those now in use would emerge from such research, and the I3P would be responsible for promulgating information on them.

Also, there is a consensus that, to bring down evaluation costs, fundamentally new tools and techniques are needed. These methodological instruments are not being developed, and evaluation costs are still too high. More R&D is needed.

5. Establish Linkages that Promote the Gathering and Sharing of Information

I3P's information sharing activity should include the product and services evaluation area. It should gather and disseminate information to support the R&D activities discussed above. It should collect and distribute information on best practices for evaluation. It should maintain an overall understanding of the extraordinarily diverse assortment of entities active in evaluation and standards setting. A fundamental policy question each year should be, "Is the currently existing patchwork quilt, overall and on balance, adequate for national security?" This answer in 1999 was certainly "no."

D. EXTERNAL RELATIONS

In fulfilling its functions in the area of product and services evaluation, the I3P would interface with a vast number of entities including: users in the critical infrastructure sectors, information technology vendors and providers, associations representing users and vendors, universities, the executive and legislative branches of the U.S. government, foreign governments, and international bodies. Governing and oversight structures for the I3P must represent a balancing of the most important of these interests; however, this does not impose demands different from those implicit in the basic R&D function.

Successful interactions with industry would be built on three qualities and capabilities of the I3P. The first is a determined and patient building of mutual confidence and respect. In order for this to succeed, the I3P must have intellectual "trading goods" in the form of internal expertise. In carrying out the gathering and disseminating of best practices, the I3P would acquire a significant satchel of trading goods. It would be providing useful tidbits regularly and would have broad knowledge about what is going on in evaluation technology and the critical infrastructure sectors. Finally an ability to

of effort if one seeks to keep disruptions localized. See National Research Council, *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, 1999.

deploy money *very* quickly at critical moments would earn it a special place among the professionals who work in user organizations, academic institutions, and research entities. Fifty or a hundred thousand dollars is very little in federal budget terms, but for these professionals getting authorization to spend that much money on something that was not pre-approved through lengthy review processes is usually out of the question. They would want to be friends of an organization that could commit such funds in a matter of hours or at most days. This last capability would be easy to establish in a private sector organization, less so in a government organization.

Chapter 9

EDUCATION AND TRAINING

The Institute for Information Infrastructure Protection (I3P) should ensure its research activities contribute to preparing the IT workforce to understand and address information infrastructure vulnerabilities. The availability of personnel trained in information assurance is essential for the protection of the information systems across the critical infrastructure sectors. A research program that is responsive to workforce needs can be successful in building a pool of qualified instructors and researchers, recruiting and training professionals, and increasing awareness in the information technology field.

Interview respondents and workshop participants emphasized that current efforts to train the workforce are inadequate to meet future needs and identified some of the needed functions. Some experts recommended that the I3P should perform many of the needed functions itself, such as curriculum development, financial support to students, and certification of professionals and programs. Others felt that the I3P should primarily offer support and resources to the outside organizations already engaged in these activities.

A. EDUCATION AND TRAINING REQUIREMENTS

1. IDA Interviews and Workshops

The PCAST proposal included training among the technical concerns to be addressed in its proposed R&D agenda. Participants in the IDA interviews and workshops corroborated the need for a range of education and training activities in information assurance. Current activities are reportedly small in scope, with perhaps as few as 20 universities and 10 federal agencies offering major information assurance training programs. Only a handful of universities offer information assurance education as part of a comprehensive teaching and research program comparable to more traditional academic disciplines.

A number of interview respondents emphasized the lack of qualified instructors as a major difficulty in maintaining a high level of activity in information assurance

education. For example, some numbered the pool of tenured professors in the U.S. who are engaged in large-scale information assurance teaching and research activities at just one dozen. The number of information assurance graduate students at research institutions is also small, and many are foreign citizens and therefore unable to work on research projects that require access to sensitive information.

Although information assurance has yet to gain recognition as a major area of research and professional activity, demand for information assurance professionals is high. Several interview respondents expressed frustration at the difficulty of finding personnel trained in this field. Some schools are reporting salary offers considerably higher than average for students graduating with experience in information assurance.¹

Career opportunities for information assurance professionals are expected to increase in the near future as more information on threats and vulnerabilities, as well as new methods and approaches for dealing with them, becomes available. However, some interview respondents indicated that better defined, higher profile career paths, especially in law enforcement and the military, are needed to encourage students and soldiers to consider careers in information assurance.

There is a need for both information assurance specialists and non-specialist practitioners in a variety of career fields. Interview respondents identified at least four types of professionals who need to be trained in the principles and practices of information assurance:

- Those who design, implement, evaluate, modify, and maintain networked systems must be trained to ensure security by design and by practice.
- Designers and engineers of widely distributed software and hardware must understand how to minimize the vulnerabilities that their products introduce into the information infrastructure.
- Managers and executives must be familiar with the technology and practices in order to coordinate the above efforts effectively.
- Computer users must understand how their actions affect security.

¹ See Computing Research Association (CRA), *The Supply of Information Technology Workers in the United States*, www.cra.org/reports/wits/chapter_1.html, October 13, 1999. (Hereinafter cited as CRA Report.)

2. Pipeline of Information Technology Workers

Information assurance workforce issues are directly related to workforce issues in the broader field of information technology. Before addressing ways to increase the 'pipeline' of information assurance workers, it will thus be useful to review the structure of IT training as a whole.

a. Degree Programs

The role of degree programs in supplying information technology workers can be described with the aid of a typology from a recent publication by the Computing Research Association. It classifies information technology workers into four categories:

- *Conceptualizers*. Conceive of and sketch out the basic nature of a computer system artifact (e.g., researcher, system architect)
- *Developers*. Work on specifying, designing, constructing, and testing an information technology artifact (e.g., system designer, computer engineer, tester)
- *Modifiers/Extenders*. Modify or add on to an information technology artifact (e.g., programmer, database administrator)
- *Supporters/Tenders*. Deliver, install, operate, maintain, or repair an information technology artifact (e.g., network administrator, computer support)²

Table 9-1 outlines the contributions of degree-granting institutions to the pipeline of IT workers, using the Computing Research Association definitions.

² Ibid., chapter 2. This section borrows heavily from the CRA report.

Table 9-1. Sources of Information Technology Workers

Degree	Job Category	Skills	Pipeline Issues
Vocational	Supporters/ Tenders	Entry-level and operating skills such as data entry	Only 1/3 of two-year colleges award IT-related degrees
Associate's (2-Year)	Supporters/ Tenders	Discipline-specific training on current software packages, operating systems, and network administration, etc.	
Bachelor's	Developers, Modifiers/ Extenders	More conceptual knowledge than specific training; able to perform more design tasks, update knowledge quickly	Largest source of IT workers; most popular choice is non-related technical major with some IT-related coursework
Master's	Conceptualizers, Developers, Modifiers/ Extenders	Combination of conceptual knowledge and specialization; research experience	Difficult to attract, retain students; 1/3 of grad students are foreign
Doctoral	Conceptualizers	Breadth of knowledge; expertise in particular area; trained to teach or carry out research	About 850 new Ph.D.s per year; almost half are foreign citizens; only 30% enter teaching

The largest source of IT workers is four-year bachelor's degree programs, but not necessarily in fields related to information technology. Most commonly, these workers have degrees in technical fields unrelated to information technology but with additional coursework or training in IT subjects.

Nevertheless, the Computing Research Association study found that several types of degree programs related to information technology are commonly available at the undergraduate level:

- *Computer engineering.* Graduates work primarily in computer hardware
- *Computer science and engineering.* Graduates work primarily in hardware, firmware, and software
- *Computer science.* Graduates work primarily in software design and implementation
- *Software engineering.* Graduates work with the engineering of software, with special attention devoted to large and critical systems
- *Computer information science.* Graduates work on the development of information systems with emphasis on information as an enterprise resource
- *Information systems.* Graduates design, develop, implement, and maintain business information systems

- *Management information systems.* Graduates design, develop, implement, maintain, and manage information systems with emphasis on the management of the systems
- *Information science.* Graduates usually work in libraries or similar facilities

In contrast to the variety of IT-related majors at the undergraduate level, the vast majority of graduate (master's and doctoral) degrees are produced in computer science departments. A number of IDA interview respondents emphasized that universities are finding it especially difficult to recruit and retain graduate students and suggested a few reasons. One is that there is fierce industry demand for highly skilled information technology workers. Another is that academic research has taken on an increasingly short-term focus and has thus become less distinguishable from industry work. A third reason is that, with increasingly heavy teaching loads, computer science faculty members have little time for advising or mentoring their graduate students.

b. Non-degree Programs

This type of training provides information technology workers with the skills needed to enter specific vocational jobs. Table 9-2 lists several types of non-degree IT programs.

Of these non-degree programs, corporate universities are perhaps the fastest growing. Despite promising activity in the non-degree sector, quality is difficult to assure. There are essentially no standards or accreditation processes in the non-degree training market.

c. Conclusions on Information Technology Pipeline

With the exception of some graduate degree programs, most types IT training and education are in high demand. However, the availability of instructors limits the number of students that can be accommodated. Excellent opportunities in industry and other factors make it difficult for institutions to attract and retain graduate students and qualified instructors. Universities currently employ a large number of adjunct faculty, but some interview respondents said that many more information assurance professionals are willing to serve as adjunct instructors. University regulations, the tenure system, low adjunct pay scales, and company policies tend to restrict the use of adjuncts.

Table 9-2. Non-degree Programs

Source	Type of Training
Vocational training schools	Vocational instruction for specific jobs in the lower-end occupations of the IT workforce.
Certificate programs at traditional four-year colleges	Aimed at college graduates looking to upgrade their skills
Four-year college course offerings	Sometimes tailored for specific companies located near the schools
Certificate programs at two-year colleges	Aimed at college graduates as well as beginning students, focus on the less skilled kinds of IT work.
Private educators	Consulting services or short courses focused on specific IT skills for every skill level and occupation
Product suppliers	Training in use of specific products, certification of technicians
Corporate universities	Companies and industries use to influence curriculum and address personnel shortages in key areas.

Source: CRA report, Chapter 6.

B. POTENTIAL REMEDIAL MEASURES

An effective response to the need for a trained information assurance workforce must accomplish both of the following goals:

- Increase the number of qualified information assurance professionals
- Establish a pool of qualified information assurance instructors at colleges, universities, and training centers

This means that the number of professionals must increase in a way that does not take talent away from teaching. In fact, the number of teachers must also increase in order to train the next generation of information assurance professionals. This section discusses some of the measures that could be taken to achieve these goals.

1. Increase the Number of Information Assurance Professionals

As discussed above, interview respondents identified at least four types of workers who need information assurance training: network administrators, software and hardware designers, management, and users. In addition, information assurance specialists with cross-functional expertise are needed to analyze complex systems, identify vulnerabilities, and implement IA practices. Whereas specialist positions may require specialized college or graduate degrees, the information security training needs of

the general IT workforce are more varied and likely to include a mix of degree, non-degree, and on-the-job experiences.

College graduates constitute the largest source of IT workers; therefore, efforts to increase interest and awareness of information assurance should focus on introducing specialized information assurance courses into college offerings. In addition, information assurance topics should be incorporated into popular IT-related courses, such as computer science, software engineering, and information systems, to reach a broad audience.

Since many IT workers seek training after college, efforts to increase the pipeline of information assurance workers should also target graduate and post-graduate education as well as non-degree programs and employer-supplied training. Institutions and training centers that undertake the following activities may offer the greatest opportunity for pipeline growth:

- Target professionals looking to upgrade their skills
- Use adjunct instructors from industry, government, and other sectors
- Offer professional master's degrees
- Locate near industry centers
- Use distance learning formats
- Build corporate university programs

Opportunities for workers to participate in non-degree and employer-supplied training programs are increasing rapidly. However, some companies are reluctant to provide training out of concern that their competitors will hire away well trained workers. One way for companies to reduce this risk is to form a training consortium. For instance, through programs such as Partnering for Workforce Development, the SEMATECH consortium demonstrates an industry-supported training consortium designed to increase the pool of trained individuals through career marketing and development of faculty and curricula.³

Most interview respondents said that strong incentives for students, workers, and companies would be needed to increase the number of trained information assurance professionals. Proposed mechanisms include the following:

³ "Sematech in the Community," Semiconductor Manufacturing Technology consortium, www.sematech.org/public/community/workforce.htm, December 21, 1999.

- *Scholarships.* Most interview respondents recommended scholarships to encourage students at all levels to pursue specialized information assurance training.
- *Curriculum development.* Widely available information assurance curricular materials at all levels (even K-12) would facilitate the development of new courses and the integration of the newest information assurance principles and practices into existing curricula. Some interview respondents expressed the need for a national syllabus, but others were skeptical that courses could be developed in a timely manner. The National Science Foundation has demonstrated a method that brings faculty together with researchers in a workshop format to write curricula based on the latest research findings. These materials are then posted on the World Wide Web for instructors to use immediately.⁴ Other models of success in curriculum development are available from NSF's Division of Undergraduate Education and elsewhere.
- *Accreditation of programs.* There is a perceived need for accreditation and certification of education and training programs. The Computing Research Association report explains that the need is especially acute for non-degree training programs, for which there are essentially no quality standards.⁵ For instance, training standards could help assure a company or agency that a contractor's employees can be trusted to perform its information assurance-critical functions. At colleges and universities, accreditation criteria requiring all students studying subjects related to information technology to be proficient in information assurance principles and practices could influence the skill sets of a wide range of future IT professionals.
- *Certification of IA Professionals.* Many interview respondents stressed the importance of certifying professionals in Information Assurance. They said that certification standards that adapt quickly to the changing state of the art in Information Assurance are needed as a pool of qualified personnel develops.
- *Development as a profession.* Recognition of information assurance as a professional occupation, through professional membership societies similar to those for other professions, is vital to improving visibility and increasing interest in the field. Currently, the Information Systems Security Association fills this need. Some interview respondents suggested that a professional society may be best positioned to take a lead role in curriculum development. Some interview respondents even advocated a society to license information

⁴ Association for Computing Machinery, Special Interest Group on Computer Science Education, *Proceedings of the Twenty-ninth SIGCSE Technical Symposium on Computer Science Education*, February 25-March 1, 1998, p.378.

⁵ CRA Report, chapter 6.

assurance specialists because of the potential consequences of their work on public health, safety, and security. In the field of Software Engineering, the Association for Computing Machinery provides a model for increasing visibility and addressing licensing issues in a rising career field with its successful Committee to Establish Software Engineering as a Profession.

- *Industry participation.* Industry can make a significant contribution toward expanding the information assurance workforce by offering internships; promoting information assurance careers; and working with educators, curriculum developers, and accreditation boards. Establishing partnerships with local universities and training centers is a particularly effective method.
- *Occupational studies.* Commonly, federal IT personnel data is out of date and has classification problems, while most industry data is firm specific and proprietary.⁶ In order to assist policymakers and educational institutions in assessing national personnel and training needs, improved methods of data collecting across the many industries that employ information technology and information assurance workers are needed.

2. Establish a Pool of Qualified Instructors

Interview respondents indicated that a shortage of professors limits opportunities for university students to study information assurance. Several experts said that research grants for university faculty would help to engage more professors and instructors in information assurance teaching and research by bringing more recognition to information assurance as a field of academic inquiry. Many also said information assurance fellowships for graduate study are needed to attract a sufficient number of Ph.D. students to fill teaching positions.

However, other respondents said that fellowships and grants would not make a significant difference. Stronger mechanisms are needed to address the following challenges:

- Graduate fellowships might not find enough recipients. Due to the appeal of high-paying industry jobs, only 11 percent of computer science graduates attend graduate school in this country.⁷ With low demand for graduate study,

⁶ Ibid., chapter 10.

⁷ Ibid., chapter 5.

some fellowships in computer science today go unclaimed. Of those who complete the Ph.D., only about 30 percent choose to enter teaching.⁸

- Research grants for faculty might limit teaching activity. With a shortage of faculty in most computer science departments, professors typically carry a heavy teaching load. Information assurance research projects could take faculty out of the classroom, reducing the quality of teaching and advising in the department and/or limiting the number of students that can be accommodated.

Efforts during the 1980s to increase the number of computer science professors to meet increasing student demand illustrate both the potential and challenges of such initiatives. In 1980, while the numbers of bachelor's and master's degrees awarded each year in computer science were growing rapidly, production of Ph.D.s was stagnant at 250 per year. In order to increase the numbers of computer science professors available to meet student demand, the National Science Foundation and private companies provided graduate fellowships (some with the requirement that students enter teaching after graduation) and worked to build a first-class computing research infrastructure in academia. These efforts helped increase Ph.D. production to 1,000 per year by 1990, but not many of those doctorates chose to enter academic careers. In 1990, the number of new Ph.D.s awarded annually in computer science began to decline.⁹

In light of these challenges, then, it appears that the approach with the best likelihood of increasing the pool of information assurance instructors must do all of the following:

- Engage more professors in information assurance activities and support them in ways that encourage them to continue in academic careers
- Foster an interest in teaching among information assurance graduate students and offer special support for them throughout their Ph.D. programs
- Help to provide supplemental instructors so that information assurance professors may devote more time to research and advising graduate students

⁸ Association for Computing Machinery, Special Interest Group on Computer Science Education, *Proceedings of the Twenty-ninth SIGCSE Technical Symposium on Computer Science Education*, February 24-28, 1999, p.362.

⁹ CRA Report, chapter 8.

a. Support Professors

Academic research grants are likely to engage professors from computer science and other disciplines in multidisciplinary information assurance research and teaching activities. The grants should also be designed to encourage recipients to continue their academic careers in information assurance. Interview respondents have indicated that grants with the following characteristics could act as incentives:

- Make a long-term commitment (e.g., 5 years) as the NSF CAREER grants do (see below) but with more funding to support a professor plus graduate students for the full term
- Provide first-class computing facilities
- Support fundamental research without the expectation for short-term results
- Offer high prestige through high-level involvement with the sponsor and peer review opportunities (such as a peer-reviewed journal of information assurance)
- Include teaching requirements and incentives to help instructors convince their universities to add information assurance courses to course offerings

Interview respondents and the study group identified some other programs that could serve as models of success for efforts to increase the visibility and interest of faculty in the field of information assurance. These include the following:

- *Industry-supported department chairs.* A tangible way for industry to participate in the training of information assurance professionals is to endow teaching positions at universities, both to bring greater recognition to information assurance faculty and courses and to form partnerships with universities.
- *Faculty Early Career Development (CAREER).* These NSF awards are available to beginning faculty only. They last 4 to 5 years and offer \$200,000 to \$500,000 each. The awards are designed to have a lasting impact on the awardees' research and teaching careers.¹⁰
- *Presidential Early Career Awards for Scientists and Engineers (PECASE).* This prestigious award gives Presidential recognition to outstanding scientists

¹⁰ "Faculty Early Career Development (CAREER)," National Science Foundation, <http://www.nsf.gov/home/crssprgm/career/start.htm>, November 24, 1999.

and engineers at the outset of their independent research careers.¹¹ A similar award could bring needed recognition to the field of information assurance.

In addition, companies should exercise restraint against hiring doctorates with expertise in Information Assurance away from universities. Major companies took collective action to show similar restraint during the 1980s, but today such collective action may be difficult to achieve since companies that need information assurance professionals are scattered across many industries. A far-reaching consortium may be able to achieve effective collaboration.

b. Foster an Interest in Teaching

Information assurance graduate fellowships, by offering higher stipends and more favorable terms than other computer science support, could attract graduate students to complete the Ph.D. and enter academic careers qualified to teach in this field after graduation. Some ways in which this could be done are listed below:

- Offer greater prestige, higher stipends, and more academic freedom than other computer science fellowships¹²
- Provide assistant teaching experiences or participation in faculty preparation programs
- Require recipients to refund monies if the Ph.D. is not completed in a timely manner or if they leave graduate school to pursue industry careers
- Support students through the completion of their doctorate degrees and include incentives to enter teaching careers.

The study team and some interview respondents identified a couple of current programs as models of success:

- *Shaping the Preparation of Future Science and Mathematics Faculty.* A new NSF-supported program that aims to encourage students to consider academic careers through such initiatives as financial support for travel to academic conferences and career exploration workshops.¹³ It could have an effect if applied specifically to the field of Information Assurance.

¹¹ "Presidential Early Career Awards for Scientists and Engineers," National Science Foundation, <http://www.nsf.gov/pubs/1998/pecase98/pecase98.htm>, November 24, 1999.

¹² Setting off an "arms race" among fellowship sponsors could prove counterproductive, but information assurance fellowships should at least be "second to none."

¹³ This program is part of an existing initiative called Preparing Future Faculty, which is supported by the Council of Graduate Schools and the American Association of Colleges and Universities.

- *Research Experience for Undergraduates (REU)*: Another NSF project, this program exposes undergraduates to university research through a summer institute and could inspire interest in information assurance academic careers if specifically applied.

c. Provide Supplemental Instructors

Additional instructors and support staff in information assurance are needed at all levels. As undergraduate demand increases, professors in computer science carry an increasingly heavy teaching load that leaves them with less time to advise graduate students. In fact, according to the Computing Research Association study, the number of newly declared undergraduate computer science majors at research universities has grown at a rate of 40 percent per year since 1997.¹⁴ Universities could be encouraged to use supplemental instructors, such as professors who have retrained for information assurance and adjuncts from industry, to help introduce information assurance topics into their curricula. Support staff could be provided to assist with research-related tasks.

- *Use of adjuncts*. Interview respondents indicated that there is a sizeable number of professionals in industry, government, and other sectors who would like to help teach courses in universities, but university and company policies often prohibit them from doing so. If such restrictions were lifted, industry could become a major source of adjunct instructors, especially in locations where the local IT industry is strong.
- *Support staff*. Funding for personnel who are responsible for performing administrative tasks, maintaining laboratory equipment, and teaching undergraduate laboratories would help support university education. These personnel would give computer science professors and graduate students more time to teach, advise, and conduct research in departments with increasingly heavy teaching burdens.
- *Faculty Retraining*. This idea grows out of a program called Institute for Retraining in Computer Science (IFRICS) that took place from 1983 to 1989 and similar programs. At IFRICS, which was jointly sponsored by the Association for Computing Machinery (ACM) and the Mathematical Association of America (MAA), mathematics professors could become qualified to teach undergraduate computer science courses through two summers of intensive training. IFRICS served as a major source of instructors as the new field of computer science grew in the 1980s. The IFRICS model could be applied to information assurance, attracting faculty from

¹⁴ CRA Report, chapter 3.

mathematics, computer science, and other technical fields. Although retraining professors from a variety of fields for information assurance seems appropriate given the interdisciplinary nature of the subject, some interview respondents warned that retraining may no longer be practical because computer science has developed greatly as a discipline since the 1980s.

Increased use of retrained or adjunct faculty should not endanger the accreditation status of most universities. The Computer Sciences Accreditation Board, which is being merged into the Accreditation Board of Engineering and Technology (ABET), calls for each professor to demonstrate "at least a level of competence that would normally be obtained through graduate work in computer science," a requirement that could be filled through participation in a retraining institute. The current criteria allow supplemental instructors other than full-time faculty to teach courses but state that "full-time faculty should oversee all course work and should cover at least 70 percent of the total classroom instruction."¹⁵

C. CURRENT ACTIVITIES

There is currently no coordinated effort to address all of the needed education and training functions in information assurance. However, a number of government and private sector activities have been proposed or are already underway to focus increased attention on information assurance education, training, and personnel needs. These initiatives are small in scope and interviewees generally agreed that they do not comprise a complete solution to the problem.

1. Government Initiatives

The executive branch of the federal government is working to gain congressional approval of a plan called the Federal Cyber Services (FCS) training and education initiative. Most notable in this initiative is the Scholarships for Service (SFS) or "CyberCorps" initiative. Under this proposed program, students would receive college scholarships in exchange for a commitment to serve in federal information security positions for four years. The program would support up to 300 students per year.

¹⁵ "Computer Science Accreditation Commission (CSAC) of the Computing Sciences Accreditation Board (CSAB) Criteria for Accrediting Programs in Computer Science in the United States, June, 1996. http://www.csab.org/criteria96_2.html, November 23, 1999.

Other elements of the FCS education and training initiative include the following:

- *Office of Personnel Management (OPM) occupational study* to identify training, certification, and personnel requirements for information systems security occupational needs within the Federal Government
- *Centers for Information Technology Excellence (CITE)* to train, certify, and retrain federal information security personnel
- *High school recruitment and training initiative* to identify promising students, promote awareness, develop a Federal INFOSEC awareness curriculum
- *Federal INFOSEC awareness curriculum* to ensure the entire Federal workforce is developing computer security literacy¹⁶

The National Security Agency recently initiated a high-profile program called the National INFOSEC Education and Training Program (NIETP) to recognize universities that offer significant research and education programs in information assurance with the designation INFOSEC Center of Excellence. In order to gain that recognition, universities must meet the curriculum standards that are used for the training of federal INFOSEC professionals.¹⁷ Seven universities, listed below, have qualified for the designation:

- James Madison University
- George Mason University
- Idaho State University
- Iowa State University
- Purdue University
- University of California at Davis
- University of Idaho

Other government organizations involved in activities related to information security education and training include the following:

- *National Security Telecommunications and Information Systems Security Commission (NSTISSC)*. Develops curriculum and training standards for

¹⁶ *National Plan for Information Systems Protection*, Executive Summary, The White House, pp.28-29, <http://www.whitehouse.gov/WH/EOP/NSC/html/documents/npisp-execsummary-000105.pdf>, January 7, 2000.

¹⁷ "Centers of Academic Excellence in Information Assurance Education," NSA INFOSEC Page, <http://www.nsa.gov:8080/isso/programs/coeiae/index.htm>, November 17, 1999.

federal information security personnel and serves as a national-level forum for training issues. Also participates in a government-private industry efforts to establish training guidelines and standards and to promote sharing of information among all federal agencies.¹⁸

- *National Science Foundation (NSF)*. Executes a variety of programs related to research and education, including summer salary for investigators, support for graduate assistants, travel, and equipment. Received \$18.4 million of the \$485.2 million in the FY2000 Federal Critical Infrastructure Protection Research and Development budget,¹⁹ but these funds went to existing initiatives related to infrastructure protection rather than to introduce new information security programs.
- *Department of Defense (DoD)*. DoD places particular emphasis on training its workforce. For instance, each service plus the NSA, DIA, and DISA provide a full range of information security courses to their system and network administrators. All these plus the Defense Logistics Agency (DLA) provide information security training for Information Systems Security Managers and Information Systems Security Officers.²⁰ Still, DoD is increasingly concerned about the size, quality, readiness, and retention of its information security workforce, both civilian and military. In September, 1998, an Information Assurance and Information Technology Human Resources Integrated Process Team was commissioned to recommend mechanisms to achieve and sustain critical information security and information technology management skill sets in the Department.
- *Naval Postgraduate School*. Offers program of information security education and research leading to master's and Ph.D. degrees for officer-students.²¹

¹⁸ "NSTISSC Issue Groups," National Security Telecommunications and Information Systems Security Commission, http://www.nstissc.gov/html/issue_groups.html, November 23, 1999.

¹⁹ "Critical Infrastructure Protection: Toward an Effective Federal R&D Agenda," presentation by Bruce W. MacDonald, White House Office of Science and Technology Policy, Defense Week Conference on Defending National Critical Infrastructure, Washington, D.C., June 15, 1999.

²⁰ Information Assurance and Information Technology Human Resources Integrated Process Team, "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," Office of the Secretary of Defense, August 27, 1999.

²¹ "The NPS CISR Approach to Information System Security Education," presentation by Dr. Cynthia Irvine given at the National Information System Security Conference, Crystal City, VA, October 19, 1999.

2. Private Sector Activities

Some examples of organizations outside the government that are working to address information assurance educational and professional needs include the following:

- *National Colloquium for Information Systems Security Education (NCISSE)*. Created in 1997, NCISSE provides a forum for leading figures in government, industry, and academia to work in partnership to define current and emerging requirements for information systems security education. One goal of the Colloquium is to influence and encourage the development of information security curricula, especially at the graduate and undergraduate levels. The Colloquium web sites currently contain course materials on Ethics in Computing, Risk Management, and Malicious Logic.²²
- *International Information Systems Security Certification Consortium ([ISC]²)*. The (ISC)² is an international organization dedicated to the certification of information systems security professionals and practitioners. (ISC)² grants the "Certified Information Systems Security Practitioner" (CISSP) certification to qualified individuals. Candidates are required to pass an examination and subscribe to the (ISC)² code of ethics.²³
- *Information Systems Security Association*. International organization of information security professionals and practitioners. Provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.²⁴
- *Purdue University Center for Education and Research in Information Assurance and Security (CERIAS)*. Center for education and research in Information Assurance and Security, with activities ranging from multidisciplinary research with industry sponsors to training of specialists to public outreach.²⁵
- *James Madison University*. Offers a master's program with concentration in information security that is administered over the Internet.²⁶

²² National Colloquium for Information Systems Security Education, <http://www.infosec.jmu.edu/ncisse>, November 23, 1999.

²³ International Information Systems Security Certification Consortium, <http://www.isc2.org>, November 23, 1999.

²⁴ Information Systems Security Association, <http://www.issa.org>, November 23, 1999.

²⁵ "Center for Education and Research in Information Assurance and Security," Purdue University, www.cerias.purdue.edu, November 23, 1999.

²⁶ "Information Security Program at James Madison University," James Madison University, www.infosec.jmu.edu, December 3, 1999.

- *Armed Forces Communications and Electronics Association*. Offers one-day seminars in Information Assurance for Senior Executives.²⁷

3. Functional Gaps

A considerable gap exists between the functions currently being performed and the identified education and training needs for information assurance. First, there is a need to increase the size and scope of each of the initiatives mentioned above. Second, a considerable number of roles remain to be filled. Table 9-3 provides a summary assessment of the adequacy of existing activities.

D. THE ROLE OF THE I3P

The assessment of existing activities in table 9-3 indicates that many gaps exist in the area of educating and training the Information Assurance workforce. Although experts agree that action must be taken to address the education and training needs, they do not agree that the I3P is the best organization to perform all of the specific tasks.

Some education functions depend only on the execution of the I3P's research or require few additional resources. The I3P would be well positioned to pursue such activities, including the following:

- Offering research grants to university faculty with long-term commitments, peer review opportunities, teaching incentives, and funding for first-class facilities, support staff, and graduate students for the full term
- Making available, in a timely manner, research program products and findings to interested educational and professional organizations

A few interview respondents and workshop participants argued for the I3P to take a lead role in executing other new programs, such as developing curriculum, certifying information assurance professionals, and providing scholarship and fellowship support to students. Indeed, the I3P is well qualified to perform many of these functions because of its unique relationships with industry and government and its on-going activities in the areas of R&D, information sharing, and product and services evaluation. Still, the role of the I3P in education and training was most commonly described as bringing attention to

²⁷ "AFCEA International," Armed Forces Communications and Electronics Association, www.afcea.org, December 3, 1999.

the needs or coordinating a sustainable effort among many players, including government, industry, and academia.

Table 9-3. Assessment of Existing Education and Training Activities

Task	Existing Activities	Assessment	I3P Role
Increase Number of Information Assurance Professionals			
Scholarships	Scholarships for Service proposal	Require gov't service, not yet approved	Co-sponsor private sector scholarships
Curriculum development	NCISSE NSTISSC	NCISSE new, NSTISSC for government needs,	Provide research support, sponsor workshops
Accreditation of college and university programs	ABET will soon oversee all computer-related programs	May expand coverage, potentially including information assurance	Encourage accreditors to include information assurance
Program Recognition	NSA-NIETP	Recognition but few financial awards	Encourage and support
Accreditation or training standards for non-degree programs	NSTISSC	Essentially no accepted standards outside government	Support development of standards
Certification of IA professionals	(ISC) ²	Must adapt quickly to changing needs	Support ongoing certification efforts
Development as a profession	(ISC) ² ISSA	Need for more honors, discussion of licensing issues	Collaborate on body of knowledge, licensing issues
Industry consortia to further information assurance education	None identified	Should include training forum and Ph.D. hiring restraints	Help bring industry together
Occupational studies	OPM	Only for government	Conduct studies
Establish Pool of Qualified Instructors			
Graduate student support	NSF	Lack information assurance fellowships with specific teaching incentives	Co-sponsor suitable fellowships
Research grants	DARPA NSA NSF	Some lack long-term commitment, teaching requirement, and peer review opportunities	Shape own research grants to help retain professors
Foster interest in teaching	None identified	None identified	Promote awareness, encourage, support
Endowed chairs in information assurance	None identified	None identified	Help get industry involved
Faculty retraining	None identified	None identified	Promote awareness, encourage, support
Liberalize use of adjunct faculty	None identified	Limited by school and company policy	Promote awareness, encourage, support
Increase support staff	None identified	None identified	Add to research grants

Therefore, it is reasonable to conclude that the I3P should work primarily to identify and support the outside organizations that are best qualified to perform the education and training tasks identified. For instance, professional societies may have unique credibility among educators for developing curricula. Independent certification bodies traditionally perform professional certification. Financial support for students could come from any number of organizations in government or industry.

An appropriate way for the I3P to carry out its role is to monitor carefully the progress of outside organizations in addressing workforce needs. In order to do this effectively, the I3P will likely need to develop improved methods for collecting IT workforce data. As the CRA study reports, federal IT personnel data is outdated and has classification problems while industry data is often incomplete.²⁸ The I3P is well qualified, through its information sharing function, to collect and sanitize data on the information assurance workforce, assess educational needs, and identify training gaps.

As needs and gaps are identified, the I3P should resist the temptation to fill the gaps with its own programs. Instead, it should work to increase the size and scope of existing activities and create partnerships with organizations that can most effectively address the problems. The I3P should offer its these organizations all the expertise, resources, and incentives available, including the benefit of its ongoing activities in research and development, product and services evaluation, and information sharing. Some examples of tasks that build on these ongoing activities are listed in table 9-4.

Table 9-4. Tasks and Related I3P Activities

Task	Related I3P Activity
Workforce monitoring, development of new data collection methods if needed	Research and Development, Information Sharing
Graduate student support	Research and Development
Research grants to university professors	Research and Development
Funding for support staff	Research and Development
Curriculum development	Research and Development
Accreditation of college and university programs	Product and Services Evaluation
Accreditation or standards for non-degree programs	Product and Services Evaluation
Certification of IA professionals	Product and Services Evaluation
Training consortium	Information Sharing

²⁸ CRA Report, chapter 10.

Because of the experts' agreement over the importance of addressing these education and training needs, the I3P should consider building its own capabilities to perform some of the critical functions should outside organizations become unwilling or unable to do so.

Figure 9-1 summarizes the I3P's role in education and training.

Promote the education and training of the practitioners, educators, and researchers needed to provide information assurance for the critical infrastructure sectors:

- Monitor the ability of existing programs to meet workforce requirements
- Address shortfalls through partnerships with outside organizations or I3P activities
- Link the I3P's activities in other areas to education and training needs:
 - Speed the flow of the I3P research results to interested educational and professional organizations
 - Tailor sponsored research projects to support objective of increasing number of information assurance teachers and researchers
 - Use intramural and extramural hiring and intern policies to attract bright people to the information assurance field

Figure 9-1. The I3P's Role in Education and Training

E. OPERATIONAL MODELS

The National Institutes of Health (NIH) may serve as a useful model for designing the I3P. The NIH is a national, mission-oriented research organization that participates actively in supporting education and training activities. Mechanisms it has developed may well prove relevant for information assurance.

The NIH mission is to uncover new knowledge that will lead to better health for everyone. Some of the education and training activities that NIH performs are analogous to those proposed for the I3P, for example:

- Long-term research grants (averaging four years) for university faculty
- Graduate student support, some with incentives to complete the Ph.D.
- Workshops that bring researchers together to solve problems
- Curriculum development

NIH sets education priorities in a deliberative manner. At NIH, the Director of each institute is responsible for evaluating the opinions of numerous advisory groups. These include (but are not limited to) Congress, the administration, other federal agencies, patient organizations, and national advisory councils that evaluate trans-NIH

activities and recommend policy and budget directions. There is also ample opportunity for public input and oversight of activities.

NIH works cooperatively with other educational organizations, especially the National Science Foundation. NIH funds some education programs jointly with the NSF and operates others that are explicitly modeled after NSF programs.²⁹ It also conducts its own initiatives. The proposed I3P might operate in a similar way, cooperating with NSF in cases of common interests but sponsoring its own programs to achieve objectives specific to information assurance.

In supporting education and training, the experts indicated, the I3P should follow the Centers of Excellence approach. For example, in two existing initiatives, NSA's NIETP program and the proposed Federal Cyber Services education and training initiative, efforts are first concentrated at a limited number of institutions that have demonstrated significant information assurance activity. Rather than attempting to support activities at every institution, the I3P should first focus on centers of excellence where programs can be developed and tested. Then, efforts can be expanded to the wider community through the centers.

²⁹ "Setting Research Priorities at the National Institutes of Health," National Institutes of Health, www.nih.gov/news/ResPriority/priority.htm. November 12, 1999.

Part IV

Toward an Institute for Information Infrastructure Protection

Chapter 10

EVALUATION OF ALTERNATIVE STRUCTURES

The preceding chapters describe growing concerns among informed experts over the vulnerabilities in the nation's information infrastructures and outline the R&D and related functions they propose to better understand and address these vulnerabilities. Our interviews and workshops revealed widespread support for action.

We found mixed views among the experts, however, regarding which organization is best suited to perform the needed new functions. On one hand, many experts cite the wealth of activities that have already begun to address vulnerabilities in several infrastructure sectors, and question whether any new organization is needed. On the other hand, there is broad agreement that none of the existing organizations is focused primarily on information infrastructure protection or positioned to integrate activities across the full range of infrastructures, technologies, and functions that need to be addressed. On balance, there is a broadly recognized need for a new organization—provided it can be structured to perform this ambitious mission effectively.

This chapter examines several potentially effective organizational approaches. We evaluate the PCAST's proposed laboratory, along with three alternatives that were proposed in the course of this study: (1) a programmatic initiative by the government that would create no new organizations, (2) a new mission-focused government agency, and (3) a consortium of private sector firms or universities. We assess each of these alternatives and explain why an organization similar to the laboratory proposed by the PCAST holds the greatest promise of success.

In weighing these alternative structures we have focused on the fact that the information infrastructure is owned primarily by the private sector. Infrastructure owners and operators are ultimately responsible for correcting security deficiencies. Industry also retains the rights to the information that is essential for identifying and assessing infrastructure vulnerabilities. Extensive industry participation is therefore needed to provide an understanding of real world vulnerabilities and to disseminate vulnerability awareness information, R&D results, and other information to a wide array of infrastructure builders, owners, and operators. The task at hand requires an organization

that can respond to government needs and influence government programs while remaining closely linked to industry.

Our review began with the PCAST's proposed laboratory, which is described in chapter 1. We found broad support for the basic mission outlined in the PCAST proposal. In the course of our interviews and workshops, however, participants suggested modifications to enhance the viability of the PCAST's concept. These changes entailed increasing the emphasis on industry leadership and involvement, focusing R&D and related functions more tightly on areas not addressed by industry and government, and limiting the new entity to a small core staff combined with a strong external program. We refer to the modified proposal as The Institute for Information Infrastructure Protection ("I3P"). The I3P forms the benchmark for our assessment of alternatives.

In brief, the I3P would take the form of a private, not-for-profit organization with a senior private-sector board of directors. (A detailed concept of operations is presented in chapter 11.) It would interact extensively with private firms in both shaping and executing its program. At the same time, the I3P would receive government funds and would be chartered to support and coordinate with ongoing government activities. Some of its tasks would support the OSTP's Critical Infrastructure Protection Interagency Working Group and the NSC's National Critical Infrastructure Protection Coordinator in strategy development and planning. A relatively small in-house staff would focus on leadership, planning, resource allocation and coordination. A small amount of the I3P's functional work would be done in-house, but most would be contracted for and executed externally.

The remainder of this chapter describes the I3P and each of the three broad alternatives to the I3P that we considered in the review. We will then summarize our assessment of the strengths and weaknesses of these alternatives versus the proposed I3P.

A. PROGRAMMATIC INITIATIVE

One alternative is to increase the funding and range of functions performed by existing government organizations. Organizations that are already involved in conducting or sponsoring information assurance research or that have some responsibility for infrastructure protection would execute the enhanced program. Existing government mechanisms would be used to coordinate across these activities. This would be similar to many other government-wide programmatic initiatives, where a new program is

coordinated through existing organizations. Examples in the information technology area include High-Performance Computing and the Next Generation Internet.

In exploring this approach, we identified and assessed ongoing activities that might assume the needed new functions.

1. Coordination Activities

Two examples of existing mechanisms illustrate how a programmatic initiative on information infrastructure protection research might be coordinated.

The Critical Infrastructure Protection Interagency Working Group (CIP-IWG). The CIP-IWG is the activity that is currently responsible for coordinating federal R&D for infrastructure protection. The group is examining R&D options across several private infrastructure sectors, including Banking/Finance, Information and Communications, Energy, Transportation, and Vital Human Services, identifying high priority cross-cutting common needs and sponsoring R&D workshops. The CIP-IWG was formed by the Executive Office of the President, is chaired by the Office of Science and Technology Policy, and has representatives from the key R&D programs across the government.

The CIP-IWG is responsible for:

- Monitoring and coordinating ongoing and planned government R&D
- Fostering conditions for developing a close R&D partnership with the private sector, academia and international groups
- Facilitating transfer of technology from government agencies to the private sector

The CIP-IWG could be expanded to coordinate programs addressing all four of the functional areas outlined in Part III. One major shortcoming of this approach is that it provides a weak mechanism for integrating across programs and functions. There is no permanent staff, so only limited resources are available to it. In addition, the working group has had relatively limited interaction with industry because it has focused primarily on coordinating government programs.

National Coordinating Office for Computing, Information, and Communications R&D (NCO-CIC). A second government coordinating activity is the NCO-CIC, which provides a more substantial coordinating structure than does the CIP-IWG. The NCO-CIC has a small permanent staff and established ties with industry executives. It reports to the

OSTP and has representatives from 12 agencies. It is currently coordinating R&D programs in the following areas:

- High End Computing and Computation Working Group (HECC)
- Large-Scale Networking Working Group (LSN), and Next Generation Internet Initiative (NGI)
- High Confidence Systems Working Group (HCS)
- Human Centered Systems Working Group (HuCS)
- Education, Training, and Human Resources Working Group (ETHR)
- Federal Information Services and Applications Council (FISAC)

The NCO-CIC also supports the President's Information Technology Advisory Committee (PITAC), which comprises 26 academic and industry leaders charged with providing an independent assessment of the federal government's role in information technology R&D.

The NCO could coordinate a program for information infrastructure protection research in parallel with its ongoing activities. The functions extend beyond the NCO's usual focus on R&D, but the staff could be beefed up to handle the needed coordination activities. Establishing a permanent information infrastructure protection research program under the NCO would, in the view of many IDA workshop participants, be the best way to implement a programmatic initiative. (Note that this option differs from the establishment of a governmental mission-focused activity, as described in a subsequent section, in that the NCO would remain a coordinating activity that does not have direct control over budgets.)

2. Functional Activities

Under the programmatic initiative, functional roles would be assigned to organizations that are already performing similar functions. The leading candidates in each functional area are described in Chapters 6 through 9 and are recapped briefly in the following paragraphs. It is important to note that none of these activities spans all of the functional areas, so integration across functions would have to be accomplished through a coordinating mechanism, such as the NCO.

R&D Functional Activities. As described in chapter 6, the primary agencies funding related R&D include the National Security Agency, the Defense Advanced Research Projects Agency, the National Institutes of Standards and Technology, and the

National Science Foundation. The span of program coverage and management styles varies significantly across these agencies. Basing the information infrastructure protection R&D function within these organizations would be challenging to their cultures, because it requires a long-term programmatic focus, emphasis on technology deployment, and coverage across many disciplines and economic sectors. Many experts believe these existing programs are therefore unsuited for the information infrastructure protection R&D function.

Information Sharing Activities. Responsibility for information sharing could be assigned to the existing activities described in chapter 7. Prime candidates include the National Infrastructure Protection Center or the National Security Telecommunication Advisory Committee's National Security Information Exchange. Information sharing responsibilities could also be assigned to the Computer Emergency Response Teams. As explained in chapter 7, these activities focus primarily on operational matters, and therefore do not deal with the longer-term information required for research and development. None of these activities is positioned to exchange the kinds of information outlined in chapter 7, and under this structure they may not be able to share it with the necessary research and development activities or to protect it from disclosure in a way that satisfies private sector needs.

Product and Services Evaluation. As described in chapter 8, the National Security Agency, the National Institute for Standards and Technology, and the National Information Assurance Partnership (NIAP) have the lead government responsibility for establishing and implementing product and service evaluation technologies and methods. The concept of the NIAP provides an effective framework for product and service evaluation. This responsibility would be retained under all models discussed. In the programmatic initiative, this presents the coordination activity with the challenge of ensuring that effective ties are forged between R&D activities and the NIAP.

Education and Training. The lead candidate for this functional area under a programmatic initiative, described in chapter 9, is the National Science Foundation. As with the product and services evaluation function, the challenge is to ensure effective cross-functional linkages, in this case between the research and educational communities.

3. Assessment

A programmatic initiative is a possible mechanism for performing the needed functions. This option has been discussed extensively, and it has received considerable

support from many experts within the government, as well as from some in industry and academia. It has the advantage of being relatively easy to implement compared with the other options, but, as noted above and discussed here, it offers a relatively weak structure for integrating across activities and functions.

One preliminary question in assessing a programmatic initiative is: Do the four related information infrastructure protection functions discussed in the preceding section need to be consolidated in a single, integrated body responsible for all four functions, or could they be performed just as effectively if separate entities did them independently? In the latter scheme, testing and evaluation, for example, could be managed by the National Information Assurance Partnership, while R&D could be handled by NSF or DARPA, each in different management chains within the executive branch and under the cognizance of different congressional committees. This approach has the advantage of being relatively easy to get started; however, there was general agreement during workshops and interviews that a single, unified group needs to be created to perform the critically important, overarching task of integrating across functions. In important ways, the functions enable and draw strength from each other. A coordinated programmatic initiative, therefore, is not considered an effective way to achieve the needed degree of integration; a single, real organization is required.

Of the four programmatic information infrastructure protection functions described in chapters 6 through 9, the two that most clearly drive this requirement to create a new organization are Research and Development and Information Sharing. Perhaps the most fundamental misgiving with the programmatic initiative was the general sense that budgeting and control processes force government programs to react much too slowly to keep up with a rapidly changing information technology environment. In both areas, a strong consensus emerged that a programmatic initiative would not be able to keep up with either the pace or demand of rapidly developing challenges.

Any information sharing mechanism that operates within the government, whether as part of a programmatic initiative or as a function of a new government organization, would be likely to meet with substantial industry reticence. Industry worries that any information it may share with government might be inappropriately shared with intelligence and law enforcement agencies or (through FOIA requests) become available to commercial competitors. One of the great barriers to progress to date has been industry unwillingness to share proprietary information (especially concerning vulnerabilities) with the government or competitors.

A programmatic initiative may also be read as a sign of weak government commitment. A constant refrain in interviews and workshops was industry frustration with the nebulous and disorganized character of government programs. Even when industry wants to cooperate with government, the appropriate government entity with which to cooperate is not always clear. Moreover, programmatic initiatives often start out energetically but tend to fade as administrations and "crises du jour" change, and government efforts to date have not fostered confidence that existing activities are up to the job.

Strong integration capability is needed, but no single organization within government "owns" the problem and has the breadth of vision to tackle its complexity or even to understand what is already being done. An interagency coordination mechanism such as the NCO would be a significant improvement over the current CIP-IWG framework, but it still could not solve the ownership issue. Further, the agency most likely to take the lead in such an initiative—the Department of Commerce—is perceived as too weak in the interagency process to be a reliable steward of information assurance in the interagency process. But the agency with the most institutional clout and experience promoting and executing such initiatives—the Department of Defense—would automatically arouse suspicions of pursuing its own agenda at the expense of commercial needs. In general, there is concern that a programmatic initiative might focus on individual government agency requirements rather than tackling the needs and concerns of industry to the degree that will be required here.

Of the four organizational options, the programmatic initiative poses the fewest management hurdles to slow, or potentially block, progress. It offers the easiest, quickest, and lowest start-up cost and presents the fewest potential legal and regulatory complications. However, the very simplicity and economy of such an approach is viewed by many as a signal of a continued lack of real commitment. A government response limited to a programmatic initiative, therefore, is viewed as unlikely even to get industry's attention, much less its cooperation. As detailed above, those interviewed saw this as the weakest option from a functional perspective. Perhaps its most important disadvantage is the perception that such a programmatic initiative, lacking a centralizing and guiding advocate, would remain unfocused and stove-piped and would contribute little to the ultimate goal of integrating a national information assurance agenda across disciplines and sectors.

B. MISSION-FOCUSED GOVERNMENT ACTIVITY

A second option is to consolidate ongoing information infrastructure protection R&D activities and the three closely related functional areas (information sharing, fostering product and services evaluation, and sponsoring education and training) into a new government activity focused on the information infrastructure protection challenge. This is a natural alternative to consider: The government (as does any institution) often creates new organizations to address important challenges, employing organizational approaches tailored to suit the scope of the problem.

1. Examples

The following examples illustrate how this approach has been used in the past. They range from establishing a new agency, to establishing a programmatic office, to establishing a federated activity among existing organizations.

Agency (NASA, NIH, FEMA). The creation of NASA represents a well-known historical example of this approach. NASA consolidated ongoing activities, and brought greater focus and resources to space exploration and related activities. The National Institutes of Health is another good example of a mission-focused R&D activity. Over the years, various aspects of biological and health-related R&D have been deemed to be of sufficient scope and importance to warrant federal funding of research by Ph.D. specialists as well as physicians in a facility near the seat of government. An example of a very different nature is the creation of the Federal Emergency Management Agency. It has consolidated a range of emergency response responsibilities from across the federal government, and it coordinates a range of additional activities that remain within responsible agencies.

Office (Drug Enforcement Office and the Y2K Office). The creation of a mission-focused office, with some funding authority, provides a smaller-scale alternative to the creation of a new agency. One example is the Office of National Drug Control Policy. This office is part of the Executive Office of the President. It can fund research and development, and other functions. In addition, it has review authority over the budgets of other federal agencies with programs relating to the counter-drug mission. Another, more recent, example of this approach was the creation of the Information Coordination Center of the President's Council on Year-2000 Conversion to provide a coordinated federal approach to prepare information systems and to develop contingency responses. The office is credited with meeting the complexity of the Y2K IT challenge by inspiring

public-private cooperation. This activity has budgetary authority for addressing the mission, and it has allocated resources to agencies to address their problems.

Federated Activity. Finally, a third and weaker variant of the mission-oriented activity is the creation of a "federated" activity to provide a virtual integration of programs across existing organizations. For example, a Federated Laboratory Model has been developed at the Army Research Lab (ARL). It entails collaborative research in specified areas between the ARL and research consortia that includes government agencies, private sector firms, and universities. Five-year Cooperative Research and Development Agreements, or "CRADA's," address issues of intellectual property rights and staff rotations in ways that are satisfactory both to private participants and to ARL. The approach has been very successful in attracting industry participation. Some activity is under way in industry to review by-laws and charters for operations to create such a Federated Laboratory for information assurance.

2. Assessment

Creating a mission-focused government activity provides a reasonable alternative to the creation of a new private-sector organization. As described here, the government has often used this approach to address various kinds of emerging challenges. Creation of a new government R&D organization focused on protection of the critical information infrastructures could increase the perception of a serious commitment to solving the problems associated with information assurance. Such an organization could be structured to provide the needed breadth of vision to set a national agenda for information assurance. In some respects, starting a new government office comparable to the Y2K office or continuing the Y2K office with a new mission might be easier than establishing a comparable private sector organization.

Beyond that, however, this option would present many of the same functional limitations as would a programmatic initiative. In particular, it does not address the cultural gap between industry and government. Many see the bureaucratic politics and fiscal oversight requirements that surround government R&D as fundamentally incompatible with the business models that govern the IT and related industries. In addition, concerns over access to private information by competitors or others using the Freedom of Information Act and by intelligence and law enforcement could stifle attempts to promote information sharing between the government and private sector

businesses. While a working group in the Department of Justice is addressing the need for new legislation to alleviate these concerns, such a solution is a long way off.

A new government organization would likely face staffing problems because of its inability to offer competitive salaries, the general shortage of trained personnel with information assurance expertise, and the general perception (often expressed in interviews and workshops) that government research cannot stay on the cutting edge of a field that moves as quickly as IT. Moreover, numerous interviewees (both in and out of government) expressed the view that a government agency would be relatively costly.

Consolidating government functions in a mission-focused activity, as in the historical examples cited above, succeeds only when both the President and Congress determine to support the new activity. Otherwise, turf battles and policy debates will negate the effectiveness of the new activity. In this case, complete consolidation may be counterproductive. It could undermine existing activities at DARPA and NSA aimed at protecting the government's own systems. A new, complementary government activity for information infrastructure protection R&D—along the lines of the office models discussed above—could nevertheless help to integrate efforts within the government if it is provided adequate funding as well as support to influence work going on elsewhere in government. Even if it succeeds in integrating government efforts, however, the activity's government orientation is likely to limit its success in promoting private sector collaboration.

C. PRIVATE SECTOR CONSORTIUM

Where the two previous alternatives are largely governmental in focus, a purely private alternative is to establish a private-sector consortium to address infrastructure protection issues. This idea has received strong support in some quarters. The consortium would be a private, not-for-profit entity formed by industry and led by a private-sector board of directors. While the government might provide seed money to assist in the formation of the consortium, it would thereafter be only a research sponsor or customer, not a member.

Members would come from both the users of information infrastructure protection products and services and the suppliers of those products and services. The consortium's customers would include its members, subscribers to its services, and project sponsors. Customers and sponsors would include both government activities and private firms. For example, the government could contract with the organization to assist the CIP-IWG and

the NSC's National Coordinator for Critical Infrastructure Protection and Counterterrorism in strategy development and planning. While government funding could establish linkages between key agencies and the consortium, the bulk of the organization's funding would most likely come from the private sector, and the government would therefore have little leverage over the overall program. Hence, the term "purely private sector" is sometimes used to refer to this alternative.

1. Examples

There are several examples of consortia that illustrate this approach. These have generally been formed to address technology challenges facing a particular industry sector.

"High Tech Consortium." Cisco Systems, Motorola, Solectron, Dell, and Sun Microsystems have created the High Tech Consortium (HTC) to keep track of the Y2K compliance of major suppliers and service providers. Because the industry consists of a complex network of suppliers and distributors, it is nearly impossible for individual companies to assess the Y2K readiness of their entire product lines. The HTC used standardized tools to determine and prepare for possible Y2K disruptions. Trained representatives from HTC member companies assessed the suppliers, and shared information on the Data Sharing Service, a secure, Internet-based database.

SEMATECH. SEMATECH is a not-for-profit technology development consortium of nine U.S. semiconductor manufacturers. It was created to reinvigorate the U.S. semiconductor industry, and co-funded by government (DoD) and industry with support from the University of Texas. Key objectives are to accelerate development of advanced manufacturing technology focused on semiconductors, enhance relationships between makers and suppliers, coordinate the setting of standards, develop training programs for industry and create university centers of excellence with research grants.

Of the various models described here, the consortium is the most focused on private sector requirements. Indeed, the proponents of forming a consortium favor it because it would, by its nature, entail the close participation of industry. The shortcoming of this approach is that it may be very difficult to organize the industry support needed to implement this approach. As we noted in chapter 2, industry is looking for government to take the lead in this area.

As this section illustrates, there are a number of feasible structural approaches for performing the functions needed to strengthen information infrastructure protection. We have commented briefly on their main features. The following sections present a more complete assessment of their strengths and weaknesses.

2. Assessment

A private consortium has several apparent advantages. Most importantly, it would by its very nature require the active participation of industry. Industry leadership can be expected to shape an agenda that is both practical and responsive to the changing environment. However, many experts (including some in private industry) expressed the concern that a purely private organization would be less likely to focus on the long-term, national research problems that need to be addressed.

Industry consortia have been formed in the past to focus on pressing common problems, but their time horizon and focus has tended to be relatively near-term and understandably limited to purely commercial concerns. The need for some information infrastructure protection functions will arise from a public interest or national security perspective, and may not appeal to a purely industrial organization. The solutions to many of the more important R&D problems related to information assurance will require input from a wide variety of disciplines (including, for example, behavioral science) and will come only after a very long-term investment of time and resources and after one or more false starts. In addition, while some fruits of consortium R&D may at some point find their way into commercial products or services, other consortium efforts (and often very expensive ones, like developing test beds) would bring significant but only indirect payoffs. Further, an emphasis on near-term commercial payoffs could lead a consortium to restrict the use of its research results and the flow of information about them—an approach that directly contradicts the government's interest in wide dissemination and use for the public good. Moreover, such action might expose the consortium or its members to government or private anti-trust action.

For these reasons, the option of setting up a purely private research consortium received only limited support. The consortium model also poses some difficult management challenges. To start with, such a private consortium could not necessarily count on broadly based industry support. Individual companies might contribute human and financial resources if they perceived that a consortium product offered direct

commercial advantage,¹ but many interviewees (including a number of industry representatives) questioned whether companies would support a consortium research agenda focused primarily on longer-term "national" issues that did not promise immediately marketable results.

Finally, those interviewed generally warned that there is no reason to assume that a private consortium would be able to promote cooperation and coordinate information sharing more effectively than government. Historically, consortia have worked only when industries face pressing challenges that firms believe they cannot address effectively by working independently. Our review finds that industry does not yet feel sufficient pressure to give rise to a collective effort in this area. In fact, the cut-throat nature of competition in many of the industries involved has generated a level of intra-industry mistrust that would be extremely difficult to overcome, and which—if not countered—would doom any serious effort at meaningful information sharing. In addition, many in the government would be concerned about sharing information with a purely private consortium over which government had relatively little influence.

D. THE CASE FOR THE I3P

The I3P described at the outset of this chapter presents the best chance of avoiding the potential pitfalls of purely industry or purely government solutions. As indicated in the discussion above, a programmatic initiative suffers because it is a government solution and because it does not provide a sufficiently strong focus on information infrastructure protection R&D and related functions. A new mission-focused government activity addresses the latter problem but still carries the burden of being in the government. While a private consortium would benefit from the greater flexibility of being in the private sector, it might hold the needs of its members above the public interest in information infrastructure protection. Moreover, it might be reluctant to accept leadership from the government. What is needed is an organization that bridges the gap between these governmental and private sector models. The I3P is designed in a way that accomplishes this and resolves the concerns raised by the other models.

The relative merits of the I3P and the options discussed in the previous sections are summarized Tables 10-1 and 10-2, and discussed in the following paragraphs.

¹ As was the case with SEMATECH-funded research aimed at improving the capabilities of its members' suppliers. There was no direct commercial advantage to any member.

Table 10-1. Functional Assessment of the I3P versus Alternatives

Functions	Programmatic Initiative Only	Government Organization	Private Consortium	I 3P
Ability to Meet Cross-cutting National Requirements				
Shaping the National Agenda	<p>+</p> <p>Establishes a relatively weak public and private sector agenda-setting framework</p>	<p>++</p> <p>Strengthens coordination within the government; and establishes a clearer focus for public-private coordination</p>	<p>+</p> <p>Focuses primarily on private sector needs, and provides a weak mechanism for government involvement</p>	<p>+++</p> <p>An organization with private governance and government sponsorship provides a forum for creating a balanced national agenda</p>
Integrating Activities across Sectors and Functions	<p>0</p> <p>A programmatic initiative provides no new resources or structures for integration</p>	<p>++</p> <p>New government organization could strengthen integration</p>	<p>+</p> <p>Consortium would strengthen integration within the private sector</p>	<p>++</p> <p>Organization provides balanced public-private integration capability, but would still be one among many actors</p>
Ability to Meet National Requirements in Functional Areas				
R&D	<p>+</p> <p>National focus blurred by differences among government agencies, and the balance would be undermined by a lack of strong industry participation</p> <p>Dispersion of authority undermines responsiveness; and federal program planning and budgeting processes are often slow to react to emerging needs</p>	<p>++</p> <p>Strengthens focus within government, but a government-led effort would not elicit the industry participation needed to achieve a balanced National focus</p> <p>A lead organization could consolidate decisionmaking, but it still must work within the government's budgeting processes</p>	<p>+</p> <p>A purely private sector dominated structure would not receive the government engagement needed to achieve a balanced National focus</p> <p>As a private body, could be responsive in allocating resources to meet emerging R&D needs & fill gaps</p>	<p>+++</p> <p>An organization with private governance and government sponsorship could develop a balanced National focus</p> <p>As a private body, could be responsive in allocating resources to meet emerging R&D needs & fill gaps</p>

(Cont'd)

Table 10-1. Functional Assessment of an I3P versus Alternatives (Cont'd)

Functions	Programmatic Initiative Only	Government Organization	Private Consortium	I3P
Ability to Meet National Requirements in Functional Areas (Cont'd)				
Information Sharing	<p>0</p> <p>Would support existing and nascent information sharing mechanisms</p> <p>Structure does not address industry's inhibitions to sharing information with the government</p> <p>Competitiveness and antitrust considerations continue to inhibit information sharing among industry participants</p>	<p>+</p> <p>Lead agency should strengthen information sharing mechanism within government</p> <p>Structure does not address industry's inhibitions to sharing information with the government</p> <p>Competitiveness and antitrust considerations continue to inhibit information sharing among industry participants</p>	<p>+</p> <p>Provides no mechanism for info sharing with gov't</p> <p>A well-designed "neutral forum" could overcome industry's inhibitions to sharing data</p>	<p>++</p> <p>The I3P provides a feasible home for establishing a collaborative government-industry information exchange</p> <p>A well-designed neutral forum could overcome industry's inhibitions to sharing data</p>
Product And Services Evaluation	<p>0</p> <p>Hard to achieve inter-agency consensus on needed actions</p> <p>May not engage industry</p>	<p>+</p> <p>Could strengthen federal support for improvements in product and services evaluation methods</p>	<p>+</p> <p>Might not assure neutrality within private sector and access to government sources</p>	<p>++</p> <p>Could provide a neutral forum that attracts comprehensive participation to harmonize and upgrade practices</p>
Education & Training	<p>0</p> <p>Distributed execution across government would not strengthen integration between R&D and educational initiatives</p>	<p>+</p> <p>Could strengthen federal support for educational initiatives, but would not strengthen linkages with industry and academia</p>	<p>+</p> <p>A consortium could strengthen coordination of industry-led initiatives, but it would lack access to federal information and resources</p>	<p>++</p> <p>The organization could foster collaboration between industry and the government to support education initiatives</p>

Key: 0 = no change from status quo in supporting national needs in the functional area; + = slight support; ++ = moderate support; +++ = significant support.

Table 10-1 shows how well each model would satisfy requirements specific to the major functions, along with several cross-functional needs. For example, in the R&D functional area the table provides comments on three criteria: responsiveness, national mission focus, and integration. The crosscutting criteria assess how well each structure meets requirements for shaping a national agenda and integrates that agenda across

sectors and functions. The crosscutting functional criteria also assess how well each structure motivates strong and balanced public and private participation—a key requirement for an I3P.

Table 10-2 shows how each model would satisfy management criteria. For example, we consider how well each structure does in inducing industry involvement. We also consider staffing issues, start-up challenges, cost-effectiveness, and legal and regulatory issues.

Table 10-2. Alternatives versus Management Criteria

General Criteria/Models	Programmatic Initiative	Government Organization	Private Consortium	I3P
Ability to Engage Industry	+ Increased program funding would strengthen industry's willingness to engage	++ This option signals stronger government commitment & will strengthen industry's willingness to engage	+++ By definition this is an industry driven activity	+++ The industry-led governance structure combined with government funding support will engage industry
Ability to Build Needed Staff	+++ Limited by federal salaries, but additional personnel only needed for strengthening the government coordination mechanism	-- Limited by federal salaries; staffing a new government organization could prove quite difficult	+ Industry will staff the consortium; but incentives are weak for providing top personnel	+++ Competitive salaries may be offered, and staffing a small private activity is feasible
Ease and Speed of Start-up	+++ No new mechanisms, agencies, facilities, staff needed	+ Would require new government office	--- Would require industry initiative and negotiations	+ Would require new organization; but could be incubated in existing organizations

Key: + = slight support for the management criteria; ++ = moderate support; +++ = significant support; -- = moderately opposes the management criteria; --- = strongly opposes

The I3P would be in a better position than a for-profit private organization to undertake long-term and potentially risky endeavors without having to answer to impatient shareholders looking for quick returns on their investments. Moreover, it would be better suited than a private consortium to the kind of multi-disciplinary research approaches that most experts agree are needed in this area. Because it could draw talent from universities, private industry, and policy research institutions, the I3P also could pursue a broader and more flexible research agenda.

An I3P would enjoy similar advantages over the purely government or purely private organizational options in performing the information sharing function.

Participants in the interviews and workshops generally agreed that the fundamental (and most difficult) challenge in setting up any information-sharing regime is to gain the trust of industry. The limited success of current efforts backs up the contention of many of the interviewees that while a programmatic initiative has some potential to set up information sharing mechanisms, the disincentives to industry participation would likely remain strong.

An organization, structured as a neutral, non-profit entity, could alleviate many of those concerns by acting as an honest broker, providing guidelines concerning what kinds of information industries should collect, then gathering, sanitizing, and repackaging that proprietary information in a way that would minimize the potential risks for individual companies. However, the success of this approach would depend largely on how the I3P is staffed and what provisions it makes for protecting proprietary and sensitive information that comes into its employees' hands in the course of its work.

An I3P would be granted government authority to handle and originate classified material necessary for accomplishment of its mission.

Most interviewees conjectured that an organization would be able to (1) develop the breadth of vision to help set a national information assurance agenda, (2) build on existing government and private efforts to coordinate across sectors, and (3) offer the best chance among all the organizational options of enlisting the degree of industry support and participation that generally is seen as critical to the success of any national information assurance effort. Moreover, this new organization could be incubated in existing entities. This would help expedite the process and keep costs under control.

As a private non-profit institution, the I3P would not face the FOIA concerns that might undermine government institutions. If suitably structured and carefully managed, it could also avoid the potential for anti-trust concerns related to information sharing that a purely private consortium might face. While the shortage of qualified talent in certain areas related to information assurance would, most agreed, pose challenges in the start-up phase, establishing a small permanent staff augmented by rotating personnel from industry and academia could give the I3P the necessary professional credibility and intellectual flexibility. This would have the added advantage of balancing industry's real-world experience with the theoretical and big-picture expertise of the academic and policy communities.

E. CONCLUSION

At the outset of this chapter, we noted that private firms are the predominant owners of the information infrastructure and are therefore ultimately responsible for correcting security deficiencies. Industry also retains the rights to the information that is essential for identifying and assessing infrastructure vulnerabilities. At the same time, government responsibility for coordinating across sectors to address what amounts to a pressing national problem cannot be ignored. Motivating strong and balanced public and private participation is central to progress in this area. On balance, therefore, we concur with the opinion expressed by a significant majority of participants in IDA interviews and workshops: that an organization—very similar to the laboratory proposed by the PCAST—needs to be created.

Chapter 11

CONCEPT OF OPERATIONS

The preceding chapters have set out the reasoning for establishing the I3P for Information Infrastructure Protection and the functions it should perform. In this chapter, we outline a concept of operations for such an organization. Our focus is on the kind of private-sector organization that the assessment in the previous chapter concludes is most likely to succeed in engaging industry in support of the I3P's mission. The concept of operations presented here provides a framework and starting point for creating more detailed proposals. We describe the proposed I3P's (A) mission; (B) tasks, deliverables, and performance measures; (C) structure, and (D) sponsorship and funding. Section E reviews several alternative frameworks for establishing the I3P. Related legal issues are identified in Section F.

A. MISSION

The purpose of the I3P remains essentially the same as that originally proposed for a "laboratory" by the PCAST: "...to conduct research and develop technology that would protect our critical information and communications systems from penetration and damage by hostile foreign national or sub-national groups, organized crime, determined hackers, and from natural instabilities, internal design weaknesses or human failings that can cause major disruption of highly complex, nonlinear networks." The PCAST emphasized the need to understand a wide range of potential vulnerabilities. They must all be evaluated, their risks assessed, and mitigation strategies identified. Following is a draft mission statement:

The I3P will engage with industry, academia, and government to coordinate a national R&D program and related functions with the objective of avoiding disruptions of cyber systems that could result in catastrophic failures of the critical information infrastructure. In particular, the I3P will emphasize R&D to understand vulnerabilities in the critical information infrastructure and develop counters to a widespread, well-organized attack that could severely disrupt or damage critical systems that are essential to our national defense, economic prosperity, and quality of life.

B. TASKS, DELIVERABLES, AND PERFORMANCE MEASURES

Establishing—and then managing—the I3P will require developing plans specifying concrete deliverables and performance measures in each of the four functional areas identified in Part III of this report. This will serve to clarify the organization's various roles and show how its work relates to that of other activities and initiatives. As discussed later in this chapter, steering groups that permit consultation among industry, academic, and government experts should be formed to formulate these plans, deliverables and performance measures. To provide a starting point, Table 11-1 presents representative examples for each area.

The I3P's deliverables would take many forms—tangible and intangible, broad in scope and narrow, objective and subjective in the manner in which they may be measured. For example, the first deliverable in the Overarching Management and Leadership Function is to develop a national agenda. One measure of the contribution of this activity is the degree of acceptance of the agenda by key leaders in government and industry. The I3P must be able to shape a national agenda and broadly integrate across sectors and functions. It must motivate strong and balanced public and private participation. Overall performance will be measured by how well these essential crosscutting functions are accomplished.

Similar deliverables and performance measures are suggested for each of the other functional areas. The integration of these deliverables and the performance of crosscutting functions are central to accomplishing the I3P's mission.

C. STRUCTURE

The structure of the I3P is dictated by the need to engage industry, academia, and government to work together in identifying and addressing infrastructure vulnerabilities and threats. It is imperative that the I3P maintains effective working relationships across the wide spectrum of external communities and activities exemplified in Figure 11-1. The I3P's staffing, governance structure, sponsoring relationships, and external linkages are designed to foster the needed relationships.

Table 11-1. Representative I3P Tasks, Deliverables, and Performance Measures

Tasks	Deliverables	Performance Measures
Overarching Management/Leadership Function		
<ul style="list-style-type: none"> • Shape the National Agenda • Integrate Activities across sectors and functions 	<ul style="list-style-type: none"> • Develop an agenda • Effective integration of public and private activities led by efforts of key leaders 	<ul style="list-style-type: none"> • Acceptance of agenda by key leaders in government and industry across sectors and functions • Acceptability of the I3P as a forum for integrating national activities
Function: Research and Development		
<ul style="list-style-type: none"> • Support development and integration of national strategy <ul style="list-style-type: none"> – Define and study the national information infrastructure as an end-to-end system of systems – Track public and private sector R&D (see information sharing below) – Support the development of a national R&D agenda aimed at protecting the critical information infrastructure • Coordinate and sponsor R&D to fill gaps and shortfalls in defined areas of interest 	<ul style="list-style-type: none"> • Definition and atlas of national critical infrastructure sectors and interdependencies • Integrated knowledge base identifying R&D gaps, shortages, and opportunities • A national R&D agenda • A unified and integrated framework for IA analysis and vulnerability assessments • Research project findings and products 	<ul style="list-style-type: none"> • Improvements in the understanding of infrastructures and interdependencies • IT community recognition that gaps exist and are important to rectify • Acceptance of agenda by key leaders in government and industry across sectors and functions • Advances in understanding of infrastructure vulnerabilities • Measurable contributions from sponsored research; e.g. advances in technologies for protecting infrastructure sectors
Function: Information Sharing		
<ul style="list-style-type: none"> • Provide clearinghouse to facilitate two-way sharing of information • Collect, sanitize, analyze, evaluate, archive, and disseminate information • Coordinate across sectors and technologies to identify common deficiencies and highlight areas where R&D or other corrective action is needed • Identify and appropriately classify aggregated information that, if released, could be harmful to national security 	<ul style="list-style-type: none"> • Integrated data base on infrastructure vulnerabilities • Information necessary to execute R&D program • Dissemination process that effectively communicates vulnerability assessments and research products 	<ul style="list-style-type: none"> • Effectiveness evidenced by level of sharing activity, quality of symposia • Knowledge and resources available for specified subject areas • Useful and responsive service as judged by internal and external users, fulfillment of requests within targeted timeframes • No release of classified, proprietary or sensitive information.

Continued

Table 11-1. Representative Tasks, Deliverables, and Performance Measures (Cont'd)

Tasks	Deliverables	Performance Measures
Function: Product and Service Evaluations		
<ul style="list-style-type: none"> • Coordinate the evaluation of products and services <ul style="list-style-type: none"> – Harmonize processes and criteria used by evaluators – Facilitate on-going work and the establishment of new capabilities – Fill gaps in evaluation and accreditation areas where only the I3P is serviceable • Promote and oversee R&D to improve test methods and develop tools, metrics, and benchmarks (see R&D above) • Establish linkages for gathering and sharing of information on best practices (see information sharing above) 	<ul style="list-style-type: none"> • Harmonized best practices and standards • Documentation of standards applicability • Specialized accreditation & evaluation where needed 	<ul style="list-style-type: none"> • Success judged by quantity of products and networks evaluated, evaluators accredited, rigorous criteria and methods used, purchased products certified, certified systems passing "red team" tests • Elimination of conflicts among standards available and used as evaluation criteria • Availability of improved tools and techniques, improved testing effectiveness, time, and cost • Effectiveness evidenced by membership, level of activity, increased use of best practices • Absence of unnecessary duplication
Training and Education		
<ul style="list-style-type: none"> • Promote the education and training of IA practitioners, educators, and researchers <ul style="list-style-type: none"> – Monitor the ability of existing programs to meet workforce requirements – Address shortfalls through partnerships with outside organizations or I3P activities – Link the I3P's activities in other areas to education and training <ul style="list-style-type: none"> – Speed the flow of the I3P's research results to IA curriculum, training & standards – Tailor sponsored research projects to help increase the number of IA teachers & researchers – Use intramural and extramural hiring and intern policies to attract bright people to the IA field 	<ul style="list-style-type: none"> • Curriculum specifications • Defined training programs for IA professionals • Status reports on national education and training activities • Transfer of research findings for use in education and training 	<ul style="list-style-type: none"> • Quantitative and detailed knowledge of workforce supply pipeline and demand • Measured contributions to reducing shortages, improving curricula, expanding professional certifications • Speed and effectiveness for transferring research results to educational materials • Numbers and types of professors and students supported, duration of support • Numbers and progress of recruits from outside the field

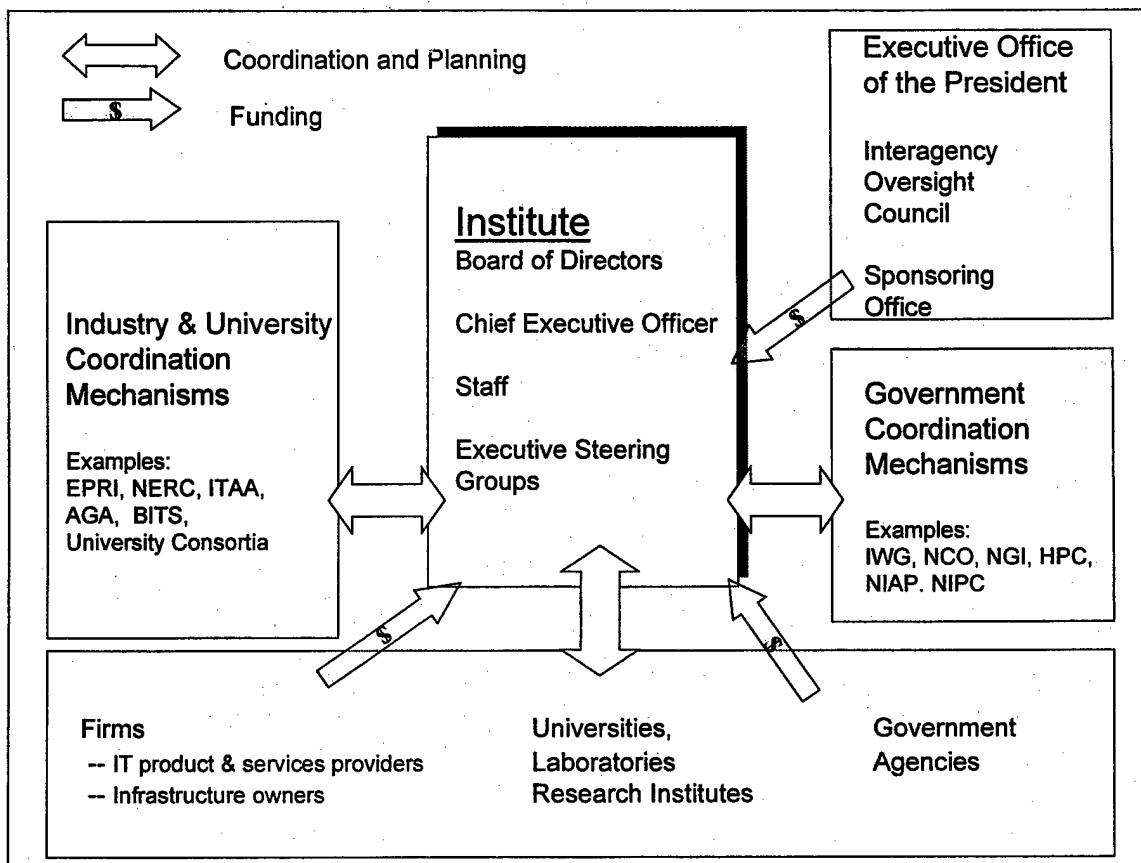


Figure 11-1. I3P Structure and External Relationships

1. Staffing and Governance

Industry officials told us that strong private sector leadership and direction from key industry CEOs is most conducive to securing effective private involvement. A prerequisite for this will be to recruit senior executives to serve on the I3P's board of directors. Industry officials have indicated that senior executives would be willing to serve on the board if it interacts with the most senior levels of government and has significant influence in shaping the I3P's program. The directors will be selected from key CEOs representing a cross-section of information infrastructure provider and user industries, along with academic and national security policy experts. The board will interact with (and perhaps have overlapping membership with) senior advisory groups whose mandates encompass infrastructure protection. These include the President's Committee of Advisors on Science and Technology (PCAST), the National Infrastructure Assurance Committee (NIAC), and the National Security Telecommunications Advisory

Council (NSTAC). Such dual-hatted relationships will strengthen the coupling between the board and national policymakers.¹

The Chief Executive Officer of the I3P, who could either be chosen by the board of directors or appointed by the President, should be a highly respected person with national stature. The CEO must be able to interact as a peer with the other members of the board of directors. The CEO also must be able to attract energetic, capable individuals to the I3P's staff. He or she must also be capable of exerting influence with the top-level officials of the Executive Branch and with members of Congress.

The I3P staff would be limited in size and would focus on strategy, planning, resource allocation, coordination, and building external relationships. The exact size of the staff will remain to be defined when detailed proposals are developed. The full-time, professional staff is expected to number between 20 and 50 people. A strong technical staff will be necessary to serve the I3P's planned functions effectively. The technical staff will engage with industry, academic, and government executives in strategy formulation, program planning, and program execution. They will be expected to

¹ Another approach is to have the board appointed by and reporting directly to the President. This could be done if the Institute were established as a public corporation. Establishing such close ties with the government under other arrangements would likely require compliance with the requirements of the Federal Advisory Committee Act.

FACA defines "advisory committee" as:

[A]ny committee, board, commission, council, conference, panel, task force, or other similar group, or any subcommittee or other subgroup thereof...which is

- (A) established by statute or reorganization plan, or
- (B) established or utilized by the President, or
- (C) established or utilized by one or more agencies,

in the interest of obtaining advice or recommendations for the President or one or more agencies or officers of the Federal Government, except that such term excludes...any committee which is composed wholly of full-time officers or employees of the Federal Government.

An I3P board that is subject to FACA would face the following requirements:

1. Its establishment would have to be determined to be "in the public interest."
2. Its membership would have to be "fairly balanced in terms of the points of view represented and the functions to be performed."
3. Its status and the need for its existence would be subject to periodic review.
4. Its meetings would have to be open to public observation unless the public interest requires otherwise and discussion or disclosure of classified information, proprietary information, or other information of a kind protected from public disclosure were involved.

organize and direct teams of government, industry, and university experts assembled to perform specific tasks.

The professional staff would be augmented in two ways. First, information assurance experts on temporary assignment to the I3P will support specific projects. Such assignments are intended help keep the I3P integrated with industry, academic, and government R&D programs and ensure that its project teams maintain technological currency. Such experts may also serve on the professional staff of the I3P for limited periods.

Second, a steering group will be established to support planning and program definition for each of the I3P's four functions. These steering groups would be responsible for integrating private and federal efforts in each functional area. For example, the R&D working group should focus on setting the R&D agenda for the I3P. It should include Chief Technology Officers (CTOs) from industry, along with academic experts and government and executives.

These steering groups will advise the I3P's CEO on overall strategy and plans for the I3P. They will perform their roles under the policy guidance of the board of directors and the direction of the CEO. The steering groups will advise in structuring specific tasks, and their members should have the authority to commit personnel from their organizations to participate on project teams. Steering group members will perform their duties on a part time basis, relying primarily on electronic communications with occasional face-to-face meetings.

An administrative staff that will operate the I3P and manage the business and legal aspects of the I3P's extensive external contracts will support the technical staff. The size of staff required for these functions will depend on the administrative approach adopted by the I3P. Needed support may be hired by the I3P, obtained through out-source contracts, or provided through matrix-support from a parent organization.

2. External Relationships

Several kinds of external relationships must be developed by the I3P in order to carry out its mission. These are shown in Figure 11-1 and described here.

- *Executive Office of the President.* The I3P must establish close working relationships with the Executive Office of the President, including the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget. Each of these offices has

responsibilities related to the mission of the I3P. The National Coordinator for Critical Infrastructure Protection and Counterterrorism in the National Security Council has specific responsibilities in this area.

There are, in addition, external advisory groups with related responsibilities. These include the PCAST, the NSTAC, and the newly created National Infrastructure Assurance Council (NIAC).

- *Industry Coordination Mechanisms.* A number of industry trade associations and collaborative activities are concerned with information infrastructure protection. The members of these organizations generally represent a broad cross-section of the respective sectors. Some examples include the Information Technology Association of America (ITAA), the Electric Power Research Institute (EPRI) and the Banking Industry Technology Secretariat (BITS).
- *Government Coordination Mechanisms.* The Critical Infrastructure Assurance Office (CIAO), the Interagency Working Group on Critical Infrastructure Protection (IWG-CIP), the National Coordination Office (NCO) of the Office of Science and Technology Policy and the Defense-Wide Information Assurance Program (DIAP) are all working to identify and coordinate research and development activities within the federal government.
- *Industry, Academic, and Government Functional Activities.* The I3P must define roles in each of its four functional areas that complement and integrate the existing related activities. The key industries include the developers of information products and services, information infrastructure owners and operators and the companies that rely on the infrastructure to conduct business. The I3P also will need the cooperation of government agencies and activities in order to obtain a comprehensive understanding of threat capabilities and intentions, identify gaps in the overall government and industry R&D effort, coordinate R&D and facilitate the transfer of technology and information.

IDA's review suggests that it is possible to establish the needed ties with each of these communities. As discussed above, relationships with industry will be built through the governance structure of the I3P, and through the execution of its functions. Relationships with the Executive Office of the President will be forged through the sponsoring relationship between the government and the I3P. (This will be discussed in the following section.) Coordination with existing private and academic coordination bodies, and with other research institutes and universities can be accomplished through the day-to-day execution of the I3P's program. It is anticipated that the I3P will

collaborate in funding and executing R&D projects with such organizations, and will also establish information-sharing activities with them.

D. GOVERNMENT FUNDING AND SPONSORSHIP

The I3P will target its research and development agenda toward areas where there currently are gaps. These gaps include important long-term research questions and broad systems-of-systems areas where industry executives believe they cannot quickly and profitably exploit the results. There is widespread agreement that research such as this requires the support of the government.

Although this study has not focused on specific funding needs, the PCAST's proposed target of \$100 million per year in government funding seems appropriate for establishing a critical mass of effort. This core level of support should be provided as general institutional funding to be allocated by the I3P staff under the direction of its private-sector board of directors. This level-of-effort funding approach would provide the I3P with the sustained support needed to plan and execute an effective program, along with the flexibility needed to allocate funding to emerging needs and opportunities.

The I3P's charter should also permit other government agencies or private firms to support specific tasks. Industry executives indicated that they would support projects on a cost-sharing basis if attractive projects with specific deliverables are defined and the firms' participation makes sense from a business standpoint. The conditions for accepting funding should be stipulated in the I3P's charter, and the board of directors should review the I3P's practices.

The sponsoring relationship between the government and the I3P would create strong working relationships. The I3P would receive its government funding and liaison support from a sponsoring organization in the Executive Branch. There has been much discussion of where this office should be located. The approach recommended by most functional experts is to locate the office in the Executive Office of the President. This approach emphasizes the inter-agency character of the I3P, and reduces the potential for turf battles.

The President's Council on Year 2000 Conversion provides a recent example of a new interagency initiative funded through the Executive Office of the President. It was established to organize and lead the government's efforts to bring the Nation's information systems into compliance with Y2K requirements. This activity had a very

small central staff and a separate budget, which it was able to allocate among government agencies responsible for executing various Y2K-related functions. A similar funding and administrative mechanism could be established for information infrastructure protection activities as well. This would create strong sponsorship for information infrastructure protection, and create a framework capable of spanning the concerns of individual governmental activities.

The sponsoring office might alternatively be placed in an existing R&D organization. The advantage of this approach is that the sponsoring office would reside within a larger organization that can contribute continuity and program management capabilities. A number of potential government hosts have been proposed and discussed. DARPA, NIST, and NSF all have administrative capability and the experience in working with the private sector appropriate to this role.

The second important linkage with the government is through the creation of an interagency oversight and coordination council responsible to review the I3P's budget and broad programmatic priorities. The council also would be responsible for promoting effective working relationships between the I3P and relevant government agencies. The council would include representatives from the National Security Council, the Office of Science and Technology Policy, the Office of Management and Budget, the Commerce Department, the Defense Department, the National Science Foundation, and other agencies with responsibilities related to information infrastructure protection.

A third mechanism for government linkage is through the government's sponsorship of specific tasks to be performed by the I3P. The I3P could be tasked, for example, to support the National Coordinating Office for Computing, Information, and Communications (NCO-CIC). This body is currently the lead activity for coordinating government-wide IT R&D. The I3P could interact with the NCO-CIC's Subcommittee on Computing, Information, and Communications R&D, which coordinates with the Departments and Agencies of the Federal government. Similarly, the I3P may perform tasks in support of the National Coordinator for Information Infrastructure Protection and Counterterrorism, the President's Advisor for Science and Technology Policy, or for government agencies.

E. ALTERNATIVE STRUCTURES

A private-sector I3P could be established in a number of ways. Three possible models were most frequently suggested in our discussions. Each of these models

includes a government sponsoring activity and a contract with a private-sector organization. The three models are (1) a private corporation such as the IN-Q-TEL Corporation recently established by and for the Central Intelligence Agency, (2) a Federally Funded Research and Development Center (FFRDC) such as those that have served DoD since WWII, and (3) a public corporation such as the the Communications Satellite Corporation (COMSAT).² Each model is discussed in turn.

1. A Private Corporation: IN-Q-TEL

The most direct method for establishing a private-sector I3P is for a government sponsor to engage in a long-term contract with a privately-formed corporation that is dedicated to the infrastructure protection mission. Many firms possess the needed technical expertise, and are actively engaged in this area. However, these firms are profit-making enterprises, and competitive considerations within their client bases, and across firms, would prevent them from performing the I3P's functions. One model that does have promise is to create an entirely new entity designed specifically to perform these functions. The CIA's recent initiative to establish a new information technology research activity, originally called IN-Q-IT, but now known as IN-Q-TEL, provides an example of how this might be done.

IN-Q-TEL is a collaborative venture among the government, industry and academia. It has a twofold mission:

- To accept strategic problems and develop a portfolio of innovative and unconventional information technology solutions, ranging from exploration to demonstration
- To fuel private research, development and application of information technologies of strategic national interest for the benefit of all partners

In undertaking these missions, IN-Q-TEL will marshal the full range of private sector IT resources on CIA's behalf and with CIA's initial funding. It will partner and

² A fourth model raised by a few experts would establish a structure akin to those employed by the Department of Energy's National Laboratories. The National Laboratories possess multi-billion dollar government-owned research facilities, which are managed and operated by contractors. Because the I3P will be a very small organization, without major facilities, this structure offers no advantages. Moreover, such a structure would inhibit the work of the I3P by making the government an interested party to agreements between the I3P and private firms or universities, which would block the creation of needed relationships. Thus, although the National Laboratories contain vital research assets, their structure does not provide a good model for establishing the I3P.

collaborate with traditional contractors as well as small "garage start-up" ventures and foreign IT companies. Over time it is expected to undertake a mixed variety of projects to include:

- Basic and applied research, engineering and development of IT-related products and capabilities to the demonstration point;
- Identification of commercial products that could be used or modified to meet needs;
- Technology surveys, product demonstrations, white papers, proofs of concept, operational prototypes, and technology forecasts.

A major strength of IN-Q-TEL is that it employs an innovative contractual mechanism that eliminates many restrictive legal and regulatory requirements that would undermine the intended mission.³ The IN-Q-TEL Corporation is being set up as a not-for-profit (501(c)) corporation independent of the CIA. Its association with the CIA is open, and all work will be unclassified. CIA is to furnish venture capital to develop ideas, products, and solutions in a range of information technology areas. IN-Q-TEL is envisioned as a technology broker and knowledge management company. The Corporation will form about 10 partnerships with industry and academia to work on specific problems.

The advantage to CIA is the ability to reach companies and universities previously out of reach because of private corporation concerns about government controls and security restrictions. Moreover, foreign nationals may be used, and there should be greater speed and agility in working problem solution paths than is ordinarily the case. In summary, IN-Q-TEL will operate in an unclassified environment, use simplified contracts, be able to employ non-U.S. citizens, have access to the best and brightest in the field, and be free to market and share R&D results.

IN-Q-TEL has established an effective contractual regime to deal with many of the legal and regulatory barriers to public-private collaboration, including intellectual property rights, information protection, and profit sharing⁴. Its proponents believe that

³ In 1989, Congress granted DoD authority (codified at 10 USC § 2371) to enter into agreements, called "other transactions," that are not subject to most of the statutes and regulations applicable to procurement contracts, grants and cooperative agreements. The CIA used a similar type of contract to create IN-Q-TEL.

⁴ Section F explores the primary legal concerns in greater depth.

IN-Q-TEL's contract will allow it to operate much as any other fast-moving high-technology company.

2. DoD Federally Funded Research and Development Centers (FFRDCs)

FFRDCs provide another feasible framework for performing the I3P's functions.⁵ They are established by contract between a sponsoring agency and the FFRDC operator, usually a not-for-profit corporation or a university. The DoD Management Plan for FFRDCs specifies a core activity that represents the principal role for each FFRDC, describes its strategic relationship with its primary sponsor, and sets out its missions, general scope of effort and core competencies. This arrangement has succeeded in achieving the needed balance between independence from the government, and the ability to work closely with both the government and private industry.

FFRDCs are already addressing infrastructure protection issues. Nearly every FFRDC has contractually defined core competency areas that touch on national information infrastructure protection. Two whose current core areas are most directly relevant to the mission of the I3P are the Software Engineering Institute, operated by Carnegie Mellon University, and the DoD C3I FFRDC, operated by the not-for-profit MITRE Corporation.

⁵ FFRDCs are defined by the Federal Acquisition Regulation (FAR) as follows:

35.017 Federally Funded Research and Development Centers.

(a) Policy. (1) This section sets forth Federal policy regarding the establishment, use, review, and termination of Federally Funded Research and Development Centers (FFRDCs) and related sponsoring agreements.

(2) An FFRDC meets some special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources. FFRDCs enable agencies to use private sector resources to accomplish tasks that are integral to the mission and operation of the sponsoring agency. An FFRDC, in order to discharge its responsibilities to the sponsoring agency, has access, beyond that which is common to the normal contractual relationship, to Government and supplier data, including sensitive and proprietary data, and to employees and facilities. The FFRDC is required to conduct its business in a manner befitting its special relationship with the Government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency. It is not the Government's intent that an FFRDC use its privileged information or access to facilities to compete with the private sector. However, an FFRDC may perform work for other than the sponsoring agency under the Economy Act, or other applicable legislation, when the work is not otherwise available from the private sector.

(3) FFRDCs are operated, managed, and/or administered by either a university or consortium of universities, other not-for-profit or nonprofit organization, or an industrial firm, as an autonomous organization or as an identifiable separate operating unit of a parent organization.

(4) Long-term relationships between the Government and FFRDCs are encouraged in order to provide the continuity that will attract high-quality personnel to the FFRDC. This relationship should be of a type to encourage the FFRDC to maintain currency in its field(s) of expertise, maintain its objectivity and independence, preserve its familiarity with the needs of its sponsor(s), and provide a quick response capability.

An illustration of how existing FFRDCs might collaborate to establish an entity with many of the elements of the proposed I3P is provided by the joint SEI, MITRE, and RAND Corporation proposal to establish a National Infrastructure Assurance Institute (NIAI). The proposed NIAI would be chartered as a not-for-profit corporation, under the direction of a board consisting of industry CEOs, the heads of consortium members, and prominent policy leaders from outside the government. Staffed by a permanent FFRDC staff, NIAI's technical excellence would also be enhanced by industry affiliates and government temporary staff, thereby affording access to industry, government, and university expertise.

3. A Public Corporation

The third mechanism is to create a federally chartered public corporation. This approach has been used on numerous occasions by the federal government to create organizations that focus on specific functions. Examples include financial organizations such as Fannie Mae and Freddie Mac. In the technology area, the Communications Satellite Corporation (COMSAT) was established as a public corporation to operate communications satellites and to serve as the United States representative to the International Telecommunications Satellite Consortium (INTELSAT).

An important feature of this approach is that it provides a legislated relationship between the I3P and the federal government. Establishing a public corporation is responsive to the recommendation of many experts that the I3P's board of directors be required to report to the President of the United States, in a manner similar to that of the National Security Telecommunications Advisory Committee. This would help to underscore that the I3P has the strong support and involvement of the highest levels of the U.S. Government. It may also be legally permissible for government employees to serve as members of the I3P's board, should that kind of close link to a particular government agency be deemed desirable.

To create such a relationship requires congressional action. Under this approach, the I3P would be a not-for-profit corporation, chartered by an act of Congress that also authorizes the President of the United States to appoint its board members. For example, the Communications Satellite Act of 1962,⁶ which created the Communications Satellite Corporation, provided that:

⁶ Pub. L. 87-624.

The corporation shall have a board of directors consisting of fifteen individuals who are citizens of the United States, of whom one shall be elected annually by the board to serve as chairman. Three members of the board shall be appointed by the President of the United States, by and with the advice and consent of the Senate, effective the date on which the other members are elected, and for terms of three years or until their successors have been appointed and qualified, and any member so appointed to fill a vacancy shall be appointed only for the unexpired term of the director whom he succeeds. The remaining twelve members of the board shall be elected annually by the stockholders. Six of such members shall be elected by those stockholders who are not communications common carriers, and the remaining six such members shall be elected by the stockholders who are communications common carriers....⁷

The charter of such a public corporation also could address the legal and regulatory aspects of the I3P's operation. This would have the advantage of explicitly stating those points where the I3P will operate differently than the notional entity receiving federal government funding. The possibility of specifically addressing and eliminating many of the factors that potentially inhibit industry cooperation with the I3P argues in favor of the public corporation approach.

F. LEGAL AND REGULATORY ISSUES

A number of legal issues will have to be addressed and resolved as the I3P's charter is created. These issues fall broadly into two categories:

- Legal issues arising from the four particular functions that the I3P is expected to perform.
- Legal issues associated with the proposed structure of the I3P and its planned relationship to the U.S. government.

Most of the functional issues were addressed in detail by the President's Commission on Critical Infrastructure Protection in its *Legal Foundations* series of reports. This discussion relies substantially on those reports. In many cases resolution of these issues may require legislation. Nonetheless, if congressional support is forthcoming, none should be "show-stoppers" for the establishment and operation of the I3P as proposed in this paper.

⁷ This provision is codified at 47 USC § 733(a).

Issues of executive agent law and civil service organization and salaries (Titles 5 and 10 of U.S. Code) that might have to be faced by a government agency performing the I3P's functions do not arise under the proposed structure simply because it is a private sector entity.

1. Acquisition Regulations

Most government contracts must—by law or regulation—include a variety of provisions that many private sector firms that do not routinely perform government-funded R&D find onerous and intrusive. These typically include audit requirements, restrictions on allowable costs, patent and data rights allocations that are generally regarded as inappropriate by commercial firms, restrictions on the choice of subcontractors, inspection requirements, and other provisions not generally found in agreements between non-governmental entities. Often, these regulations “flow down” to the subcontractors of the direct government contractor, thus inhibiting the establishment of relationships between the I3P and commercially oriented private firms.

Some relief from such acquisition requirements can be obtained. The Department of Defense, as discussed below, has the ability to contract for R&D activities using so-called “Other Transactions” under 10 U.S.C. § 2371. This authority has limitations, however. This suggests there may be a need for specific legislative action in the case of the I3P to make the use of such agreements workable.

2. Intellectual Property

Ownership and use of intellectual property resulting from the I3P R&D activities—both those it funds externally and those it conducts in-house—must be carefully addressed. If the I3P receives government funds, then standard government contracting rules governing ownership of patents and other intellectual property will apply unless some alternative contractual framework is provided. Those standard rules will generally permit the I3P to own what it develops, but that ownership will likely be subject to a government license of some kind. Government licenses have proven to be a deterrent to the participation of many firms in government-funded R&D. This has been especially true of particularly innovative firms like 3M or Hewlett Packard that are not traditionally government contractors.

There are some statutory provisions for DoD R&D contracting that may allow for a more innovative approach. For example, 10 U.S.C. § 2371 permits “other transactions”

that are not subject to the "normal" patent rights allocation required by the Bayh-Dole Act and that permit DoD and its contractor to reach an appropriate agreement on other "rights in technical data" as well. The implementation of the I3P's government funding must address these concerns and seek mechanisms such as that provided by 10 U.S.C. § 2371.

3. Restrictions on the Participation of Foreign or Multinational Firms

The use of government funds may entail limitations on foreign access to technology developed through the I3P. This issue may arise in a variety of forms ranging from export controls to "prudential" limitations on foreign access such as those commonly used by DARPA. Many current information assurance researchers and graduate students are not United States citizens. Limitations on foreign access to technology may limit the pool of talent available to the I3P to carry out its research agenda.

Access by foreign firms or foreign persons to technology and other sensitive information may be subject to legal or regulatory controls. A particularly difficult problem in this area is the identification of foreign firms. Many U.S. firms have substantial foreign ownership (Daimler Chrysler, as just one example). It can be difficult to arrive at a definition of "foreign company" that satisfies the needs of the current U.S. export control regime (or any reasonable successor regime).

4. Information Protection and the Freedom of Information Act

Protection of proprietary and other confidential information will be a key consideration in attaining the necessary degree of private sector participation and confidence in the I3P. In general, it appears very likely, based on comments made in the IDA interviews, that private entities will insist on restricting the I3P's ability to share private firms' information with the government for fear that having such information in government hands may lead to unwanted disclosure (to competitors, for example) via the Freedom of Information Act (FOIA).

The I3P, like any other private sector organization, will have to rely on the standard and customary forms of protection for confidential information: non-disclosure agreements and other forms of contracts that embody restrictions on the disclosure by one party of the confidential information of another. Whether other firms will be comfortable relying on these protections will depend largely on whether they perceive the I3P itself *or its employees who may have access to their information* as actual or potential

competitors. The rotation of research personnel suggested as part of the I3P structure will have to be very carefully crafted to address these possible concerns.

Another often-expressed concern in interviews was the Freedom of Information Act. FOIA applies by its terms only to "agency records"—documents (1) either created or obtained by a federal government agency and (2) under agency control at the time they are requested. The I3P, as proposed in this paper, is not an "agency" within the scope of FOIA. Whether data from its federally funded research efforts may be determined to be "agency records" requires some scrutiny.

The Supreme Court has held that data generated, owned, and in the possession of a private organization receiving a federal grant from an agency subject to FOIA were not agency records. The records in question had not at any time been obtained by the funding agency. Further, the Court held, the data did not become "agency records" subject to FOIA merely because the agency supervised the grant recipient in its use of the funds or because the agency had authority under the grant to obtain the data if it chose to do so.⁸ A U.S. Circuit Court of Appeals reached a different conclusion, however, holding that research results *were* agency records subject to FOIA, even though they had never been in the physical possession of the funding agency. In this case the contractor or grantee had acted on behalf of the granting agency and the agency had directed the creation of the data, planned to take possession of the data at the conclusion of the research, planned to publish the results, and used the information in its own published articles and policy development activities.⁹

It will be necessary to structure the I3P's charter and its processes to fit within the parameters implied by these legal rulings. Whatever fears firms or individuals may have about the I3P's ability to protect their confidential information, applicability of FOIA to the I3P itself should not be among them, provided that federal agencies funding the I3P do not attempt to exercise a significant degree of control over its research and information sharing activities.

Information sharing *with* a government agency *by* the I3P must be done within a carefully defined structure. First, it may well be that the nondisclosure agreements that the I3P must enter into if it is to be an effective vehicle for research and information sharing

⁸ Forsham v. Harris, 445 U.S. 169, 100 S. Ct. 977, 63 L. Ed. 2d 293 (1980).

⁹ Burka v. U.S. Dept. of Health and Human Services, 87 F.3d 508 (D.C. Cir. 1998)

will specifically restrict or prohibit disclosure to the government. Data shared with the government may have to be cleansed of confidential information—or of identifying information. If confidential information is shared, it could be exempted from FOIA disclosure if it is proprietary information within the definitions of FOIA's exemptions or fits another of the nine FOIA exemption categories. Many firms are unwilling to rely on FOIA exemptions, however. Significant additional work is needed to establish a viable information sharing framework. Some kind of legislation creating an explicit FOIA exemption for critical infrastructure protection information under appropriate circumstances may be desirable—or even necessary.

5. Antitrust

Antitrust considerations were raised by a number of those interviewed, but they are probably of little real concern. But again, this issue must be addressed in establishing the I3P's charter.

In the strictest sense, anti-trust liability attaches only to private (that is, without government involvement) sharing of information related to market division or price fixing. The exchange of other kinds of information among competitors will generally not raise the specter of civil or criminal anti-trust action either by the government or by private parties. That the I3P itself is not a participant in any critical infrastructure mitigates against anti-trust liability for sharing information with it. However, the small risk that does exist might arise if one or more firms is denied access to information or believes it has been denied such access. In such a case, an excluded firm might claim that it is the victim of a boycott or that it has been denied access to an "essential facility" that is necessary to conduct business. If information sharing with or through the I3P is mandated by government action, that should further lessen concerns about anti-trust enforcement arising from information sharing activities.

6. Liability

Liability for failure to disclose or inform about vulnerabilities is an area that must be addressed in the establishment and operation of the I3P. Generally there can be no liability where there is no duty, but the proposed structure may create such a duty.

Liability may also stem from the I3P's activities relating to product and services evaluation. The evaluation of products and services for information infrastructure protection by a private entity such as the proposed I3P probably raises no significant legal

issues. However, in those few instances in which the I3P does perform evaluations, or accredit evaluators or validate their tests (which should occur only in cases of need where no alternative is reasonably available), there may be liability issues related to reliance on the I3P's evaluations, accreditations or validations by others. However, in part because of the proposed close ties between the I3P and the government, a number of potential issues should be considered and dealt with in establishing the I3P and in designing the processes under which it will conduct itself in any case in which it becomes involved in accreditation, evaluations or validations. These should include:

- The availability of mechanisms for assuring that the processes for determining which products and services are evaluated be without bias.
- Attention to the possibility of liability resulting from testing and evaluation. It must be clear in all evaluation agreements, for example, that the government will not be held liable for the actions of the I3P or its subcontractors.
- Consideration for possible liability for "product defamation" under various state laws for the publication of negative evaluation results.
- Ownership and access to evaluation results and rules and procedures for their dissemination.

This broad concept of operations builds on the PCAST's proposal for a new laboratory and the ideas and concerns shared with the IDA review team by experts in infrastructure protection and information assurance. Based on our discussion with experts from industry, academia, and government, we believe the general approach laid out here provides the greatest chance of succeeding in fulfilling the I3P's mission.

Appendix A

The PCAST Letter to President Clinton

EXECUTIVE OFFICE OF THE PRESIDENT
PRESIDENT'S COMMITTEE OF ADVISORS ON SCIENCE AND TECHNOLOGY
WASHINGTON, D.C. 20502

December 10, 1998

President William J. Clinton
The White House
1600 Pennsylvania Avenue
Washington, D.C. 20500

Dear Mr. President:

You have made the protection of critical infrastructure a high priority, especially our interconnected electronic network which underpins our nation's monetary, national security, air traffic control, telecommunications, law enforcement, energy distribution and other such critical systems. Achieving this goal will require gaining a systematic understanding of information infrastructure vulnerabilities and developing and deploying new technology, equipment, software and procedures. We recommend the government establish and contract with a new not-for-profit laboratory, the Laboratory for National Information Infrastructure Protection (LNIIP), to create and disseminate the necessary knowledge to protect our information infrastructure. This technical organization in the private sector but with certain government oversight will complement the operational capability of the Department of Justice National Infrastructure Protection Center, created by PDD-63.

The new LNIIP should be governed by an interdependent board of directors drawn from leaders of the telecommunications, software and information technology industries and their customers, as well as from academia. The purpose of the Laboratory would be to conduct research and develop technology that would protect our critical information and communications systems from penetration and damage by hostile foreign national or subnational groups, organized crime, determined hackers, and from natural instabilities, internal design weaknesses or human failings that can cause major disruption of highly complex, nonlinear networks. This effort would include the development of a broad understanding of the robustness and resilience of such complex systems and would involve creation of means to assure graceful degradation under stress.

Information infrastructure issues affect the operations of virtually all elements of the private sector and the government. At present there is no technical organization dedicated to developing the knowledge and common technology base required to successfully address this problem and provide the basis for long term protection. The private sector does not have the incentive to develop the public knowledge and technology base required for the development of competing interoperable proprietary systems--thus federal support is needed. The justification for acquiring the needed knowledge and technology through government support of a new not-for-profit laboratory is that while most of the critical infrastructure lies outside the government, only the government is in a position to derive and make broadly available the information needed to assure the integrity of our nation's information network. Because of the complex relationships,

tight coupling between the government, information infrastructure providers and users is critical to the structure proposed to accomplish this coupling, as shown in the attached diagram.

Areas of LNIIP's technical program would include: (1) vulnerability detection and analysis; (2) security architectures and simulation systems; (3) encryption and authentication systems; (4) intrusion detection and warning systems; (5) system recovery; (6) component and software security assurance; (7) best practices for product evaluation; (8) training, and (9) human interface with complex systems. The Laboratory would also provide a linkage between government and industry and draw upon talent in academia for the purposes of: (a) serving as a clearinghouse for industry information and experience (with procedures that respect proprietary data); (b) setting and disseminating best practice information; and (c) carrying out training exercises and inspections to certify performance. The LNIIP would be concerned with creating knowledge, technology and tools; it would not be concerned with operations. We also believe that it is too ambitious to include in the baseline LNIIP charter other critical infrastructure vulnerabilities, i.e., vulnerability to terrorist chemical or biological attack, although these related considerations would necessarily play some role in the LNIIP technical program.

The LNIIP would focus on developing techniques for protection of the information infrastructure backbone; it would have the responsibility to interact with key functional areas both in government (notably defense, law enforcement, treasury, energy, transportation, and emergency services) and in the private sector (telecommunications, banking, power, airlines, manufacturing, et al). Thus, the functional industry groups and corresponding government agencies are the "clients" for the LNIIP product and must have a role in shaping the LNIIP work program.

How should the federal government accomplish coordination and oversight of the LNIIP program it sponsors while assuring that the needed close coupling with the private sector is maintained? We believe a federal council composed of those agencies that have an important interest in the information infrastructure problem is required. A federal coordinating committee acting on behalf of the council and composed of the Deputy Secretaries of Defense and Commerce and the Deputy Attorney General should provide effective management and oversight responsibility. We recommend that the Deputy Secretary of Defense chair the federal coordinating committee, although a rotating chair is an alternative.

We urge that funding for the LNIIP be placed in a budget line in the Executive Office of the President under the control of OMB and the federal coordinating committee. We recognize that this is an unusual approach; however, we believe that it is justified because circumstances dictate that government security and law enforcement set requirements for what ultimately will be the private sector's responsibility to implement its own information protection programs. A second choice might be to assign budgetary responsibility to the DOD in deference to its size, responsibility and R&D management experience. But such an assignment will cause concern both in the public and industry that DOD will wield undue influence in determining the type and degree of protection which is warranted and this approach is therefore not recommended.

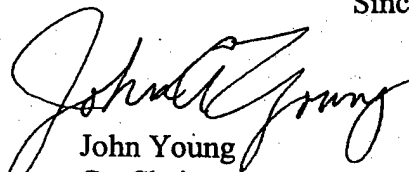
Without a specific work plan it is difficult to set a budget for the LNIIP with precision. However, we believe that about \$100 million per year would not be unreasonable after a start-up

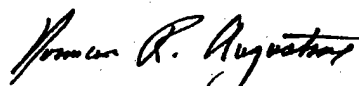
period. This money would come primarily from the federal government, although we anticipate that significant funds and in-kind support would also come from industry.

Several independent groups have proposed the creation of a new information assurance technical organization such as we are recommending here. We have endorsed this step because we believe it is the quickest and most efficient way to develop and deploy information assurance technology. In particular, we believe it is preferable to allocating to agencies, through the critical infrastructure protection (CIP) process, all available funding for information infrastructure protection. There is a need for a centrally focused effort in the private sector to develop the needed technology as quickly as possible.

If you approve, OMB and OSTP will form a small working group from DOD, DOJ, and DOC, with inputs from others, to prepare a specific proposal for your consideration for inclusion in the FY2000 budget. The PCAST Security Panel will be available to advise this working group should that be desired.

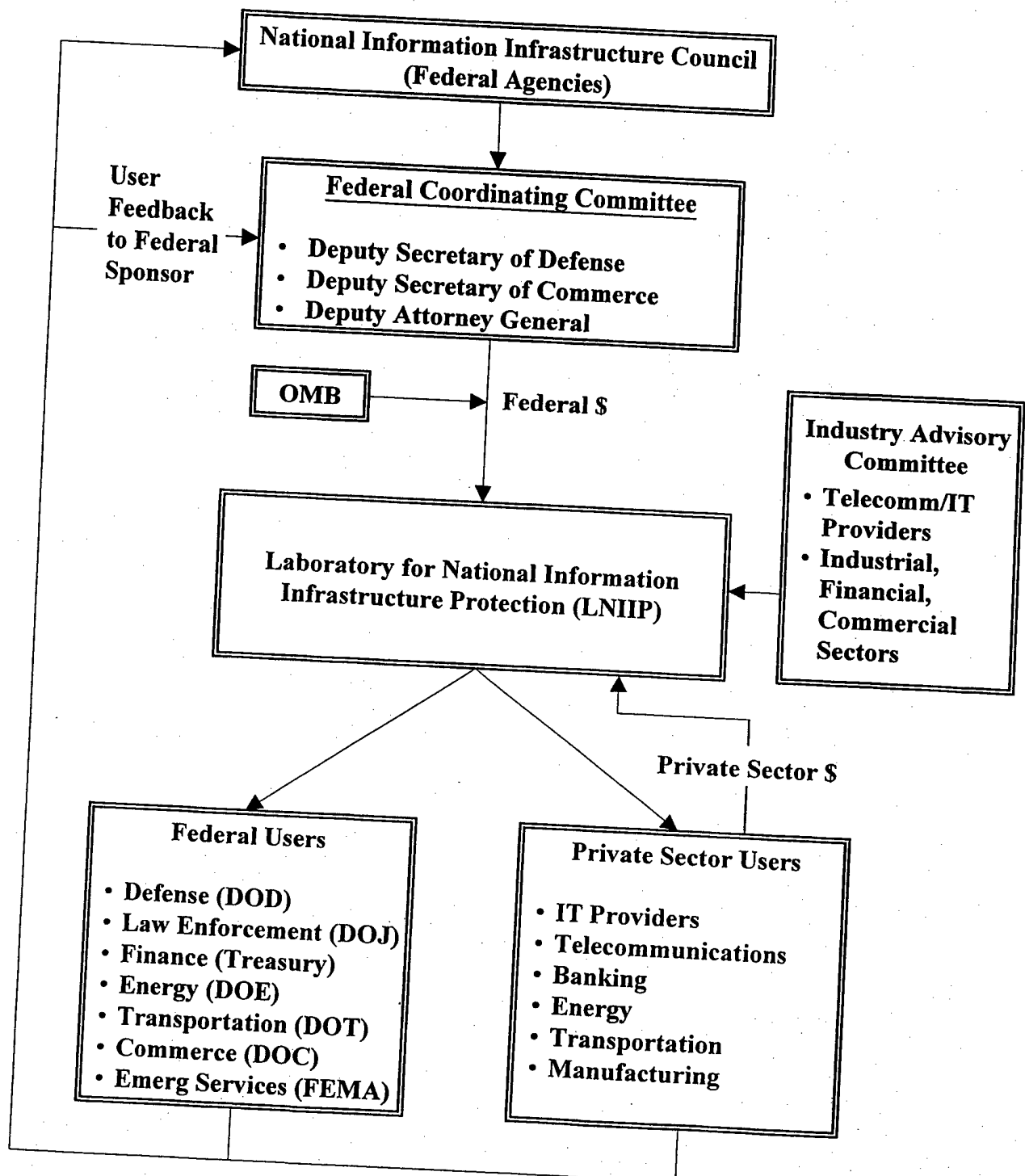
Sincerely,


John Young
Co-Chairman
PCAST


Norman R. Augustine
Chairman
Security Panel

Attachments: Proposed LNIIP Flowchart

PCAST SECURITY PANEL WORKING PAPER
Proposed Management Organization for the
Laboratory for National Information Infrastructure Protection



Appendix B

Interview and Workshop Participants

Appendix B

INTERVIEW AND WORKSHOP PARTICIPANTS

INTERVIEW PARTICIPANTS

Academia:

Duane Adams, CMU
 Rod Brooks, MIT
 Bill Dally, Stanford
 Andrew Gross, UCSD
 Mark Hill, University of Wisconsin
 Robert Hoover, University of Idaho
 Anita Jones, UVA
 Sid Karin, UCSD
 Raman Khanna, Stanford
 Tom Knight, MIT
 Steve Koonin, Cal Tech
 Alan Merten, GMU
 Robin Murphy, University of South Florida
 Geoff Orsak, SMU
 Joe Pasquale, UCSD
 Tom Perrine, UCSD
 Howard Shrobe, MIT
 Gene Spafford, Purdue
 Gary Susman, MIT
 Charles Vest, MIT

Government (& Laboratories):

Jane Alexander, DARPA
 Dwayne Allain, Rome Laboratory
 Marjorie Blumenthal, NAS
 Lee Buchanan, Navy
 MajGen Campbell, JTF CND/Space Cmd
 John Davis, NSA
 Joan Demsey, CIA
 Rick Dunn, DARPA
 Bob Eagan, Sandia
 Craig Fields, DOD
 Mike Francis, DISA
 Norman Green, CIA
 Larry Gershwin, CIA
 John Hagerling, Treasury
 Sally Howe, National Coordination Office
 Kay Howell, National Coordination Office
 Jeffrey Hunker, NSC
 Tom Kalil, Council of Economic Advisors
 Donald Kerr, FBI
 RADM Bert Kinghorn, DOT
 Ernie Moniz, DOE
 Irv Pikus, Dept. of Commerce
 Bill Press, LANL
 Fred Saafeld, Office of Naval Research
Private Sector (&FFRDCs) Cont'd:

Sami Saydjari, DARPA
 Paula Scalingi, DOE
 Richard Schaffer, DOD
 John Serbian, CIA
 Randy Shumaker, Navy Research
 Laboratory
 Sam Varnado, Sandia
 Michael Vatis, FBI
 Bill Weldon, Office of Naval Research
 Curt Weldon, U.S. Congress
 Jack Woodward, LtGen, DOD
 Rick Yanuzzi, CIA
 Robert Zomback, Army Communications-
 Electronics Command

Private Sector (&FFRDCs):

Duane Andrews, SAIC
 Bill Burnett, Gas Research Institute
 Jennifer Chayes, Microsoft
 Guy Copeland, CSC
 Steve Cross, SEI
 William Crowell, Cylink
 Jack Edwards, Nortel
 Bran Ferren, Walt Disney Imagineering
 Matthew Flannigan, Telecommunications
 Industries Association
 Jerry Gregoire, Dell Computers
 Bob Henderson, MITRE/JASON
 Stu Johnson, RAND
 Steve Katz, Citicorp
 Phil Lacombe, Veridian
 John Lane, Nations Bank
 Don Latham, Lockheed Martin
 Mike McConnell, Booz-Allen
 Gary McGraw, Reliable Software
 Technologies
 Scott Nason, American Airlines
 Rich Pethia, SEI
 Kevin Roth, ITAA
 Doug Sabo, ITAA
 Howard Schmidt, Microsoft
 George Spix, Microsoft
 Stu Starr, MITRE
 Francis Sullivan, IDA
 Lowell Thomas, GTE
 Fred Thompkins, Unisys
 Paul Tobin, AFCEA
 John Triehler, Applied Signal Technology

Terry Vickers-Benzel, Network Associates
Ken Watson, Cisco
Peter Weinberger, Renaissance
Larry Wright, Booz-Allen

Policy Community:

Norm Augustine, Lockheed Martin Corp.
Murray Gell-Mann, Santa Fe Institute
George Heilmeier, Telcordia Technologies
Robert Hermann, Global Technology Partners
Bobby Inman, formerly NSA and CIA

Paul Kaminski, formerly DOD
Tom Marsh, Air Force Aid Society
Ken Minihan, formerly with NSA
Robert Prestel, IDA Board
Don Rumsfeld, formerly DOD
Jim Schlessinger, MITRE Board
Jeffrey Smith, Arnold & Porter
John White, Harvard
Robert White, Washington Advisory Group
James Woolsey, Shea & Gardner
John Young, Hewlett-Packard

WORKSHOP PARTICIPANTS

June Workshop Participants:

Dwayne Allain, Rome Laboratory
Marjory Blumenthal, NAS
Blaine Burnham, GA Tech
Guy Copeland, CSC
John Davis, NSA
Richard L. Dunn, DARPA
Jay Gowens, ARL
Charles Holland, OSD
Robert Hoover, University of Idaho
Kay Howell, NCO
Stuart Johnson, RAND
Kathy Kincaid, IBM (ret.)
Steve King, NRL
Col. Mark Kindl, ARL
Phil Lacombe, Veridan
Steven Lipner, Mitretek
Christine McBride, DIAP
Mark Montgomery, Nat'l Security Council
Robin Murphy, University of South Florida
Rich Pethia, Software Engineering Institute,
Carnegie Mellon University
Steve Rinaldi, OSTP
Fred Schneider, Cornell University
Randall Shumaker, NRL
Stuart Starr, MITRE
David Svec, OSTP
Lowell Thomas, GTE & NSTAC
Fred Tompkins, Unisys
Terry Vickers-Benzel, NAI Labs

September Workshop Participants:

Dwayne Allain, Rome Laboratory
Frank Anger, National Science Foundation
Allan Berg, James Madison University
Guy Copeland, CSC
John Davis, NSA
Bob Eagan, Sandia
Mike Francis, DISA

Carolyn Fuller, University of Idaho
Anup Ghosh, Reliable Software Technologies
Paul Grabow, Federal Reserve Board
Bruce Guile, Washington Advisory Group
Don Hagerling, Department of Treasury
Mark Hill, University of Wisconsin
Charlie Holland, OSD
Stu Johnson, RAND
Steve Kaplan, NIPC
Bert Kinghorn, DOT
Carl Landwehr, MITRETEK
Peggy Lipps, BITS
Bruce McDonald, OSTP
Jack Marsh, College of William and Mary
Pam Martin, Int'l Computer Security Association
Christina McBride, DIAP
Gail McCarthy, EPRI
John McLean, NRL
William Mehuron, NIST
Robin Murphy, University of South Florida
Bob Nemetz, OSD
Tom Perrine, UCSD
Doug Perritt, NIPC
Rich Pethia, SEI
Steve Rinaldi, OSTP
Ron Ross, NIST
Keven Roth, DOE
Doug Sabo, ITAA
Phyllis Schneck, Georgia Tech
Randy Shumaker, NRL
Gene Spafford, Purdue
Craig Swietlik, Argonne
Peter Tippitts, Int'l Computer Security Association
Paul Tobin, AFCEA
Terry Vickers-Benzel, Network Associates
Ken Watson, Cisco